

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-007849
(43)Date of publication of application : 12.01.2001

(51)Int.Cl. H04L 12/56
H04L 9/10
H04L 12/46
H04L 12/28
H04L 12/66

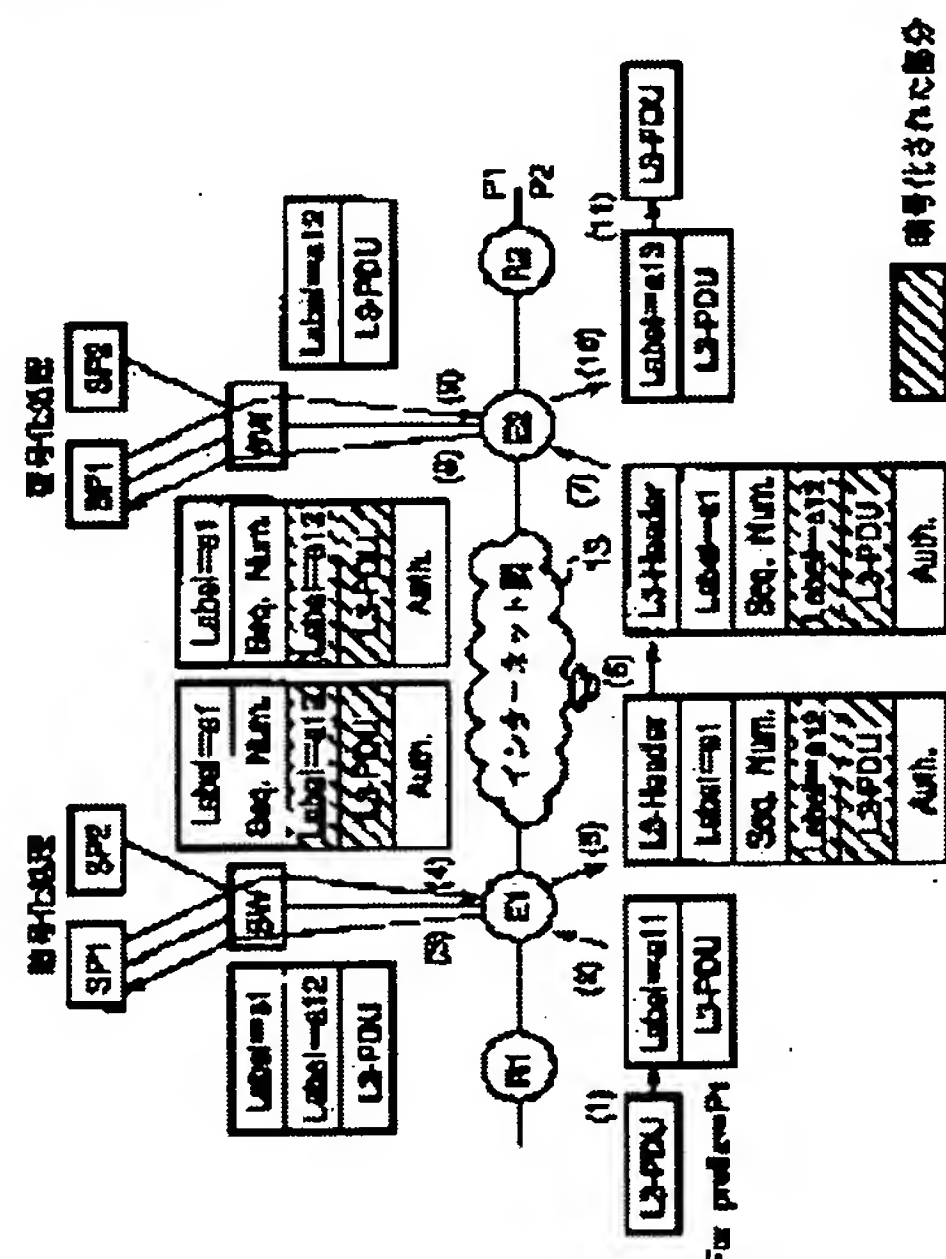
(21)Application number : 11-173022 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 18.06.1999 (72)Inventor : NOGAMI KAZUO
OBA YOSHIHIRO
KISHIGAMI TORU

(54) MPLS PACKET PROCESSING METHOD AND MPLS PACKET PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an MPLS packet processing method that can support an MPLS security function even in the case that one node supports an IP encapsulation or a plurality of VPNs realized by an LSP of the MPLS.

SOLUTION: A label switch path is set between two nodes that support a label switch, either of the two nodes encrypts a packet and uses the label switch path to transmit an encrypted packet, the other decodes the encrypted packet received on the label switch path in this encrypted packet processing method adopting a multi-protocol label switch(MPLS), where information relating to packet security association is used for the label of the MPLS to transmit packets.



LEGAL STATUS

[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2001-7849

(P2001-7849A)

(43)公開日 平成13年1月12日(2001.1.12)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L	12/56	H 0 4 L 11/20	1 0 2 A 5 J 1 0 4
	9/10	9/00	6 2 1 Z 5 K 0 3 0
	12/46	11/00	3 1 0 C 5 K 0 3 3
	12/28	11/20	B
	12/66		

審査請求 未請求 請求項の数12 O L (全 20 頁)

(21)出願番号 特願平11-173022

(22)出願日 平成11年6月18日(1999.6.18)

特許法第64条第2項ただし書の規定により図面第17図の一部は不掲載とした。

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 野上 和男

東京都日野市旭が丘3丁目1番地の1 株
式会社東芝日野工場内

(72)発明者 大場 義洋

東京都日野市旭が丘3丁目1番地の1 株
式会社東芝日野工場内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

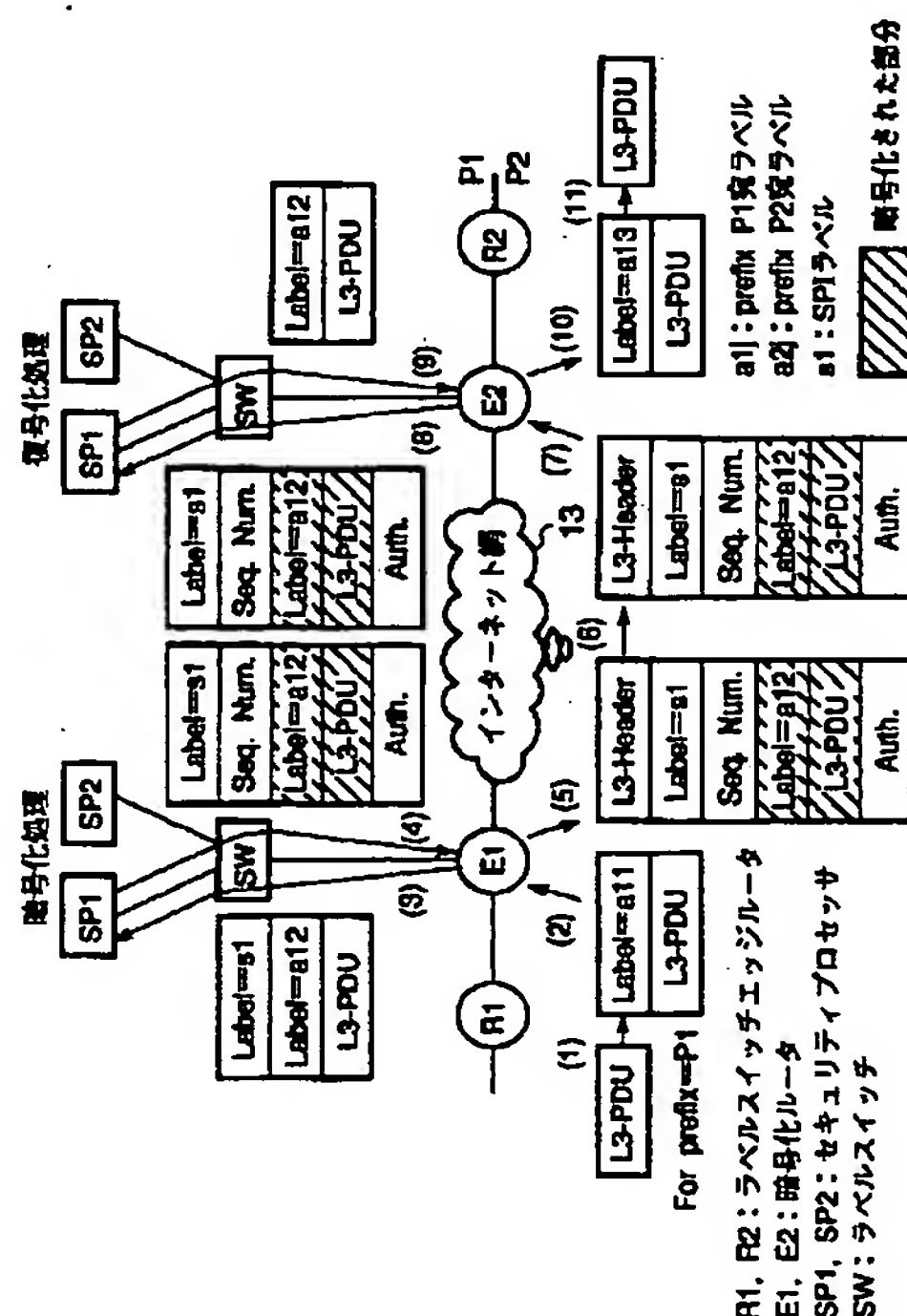
最終頁に続く

(54)【発明の名称】 MPLSパケット処理方法及びMPLSパケット処理装置

(57)【要約】

【課題】1つのノードがIPカプセル化あるいは、MPLSのLSPで実現される複数のVPNをサポートする場合でも、MPLSセキュリティ機能をサポートすることができるMPLSのパケット処理方法を提供する。

【解決手段】ラベルスイッチをサポートする2つのノードの間にラベルスイッチングパスが設定されており、2つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング(MPLS)の暗号化パケット処理方法であって、パケットのセキュリティアソシエーションに関する情報を、MPLSのラベルとして用いてパケットの送信を行うようにする。



【特許請求の範囲】

【請求項1】 ラベルスイッチをサポートする2つのノードの間にラベルスイッチングパスが設定されており、2つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング(MPLS)のパケット処理方法であって、パケットのセキュリティアソシエーションに関する情報を、MPLSのラベルとして用いてパケットの送信を行うようにしたことを特徴とするMPLSパケット処理方法。

【請求項2】 前記セキュリティアソシエーションに関する情報を表すラベルを含むパケットをレイヤ3パケットにカプセル化したことを特徴とする請求項1記載のMPLSパケット処理方法。

【請求項3】 上記セキュリティアソシエーションに関する情報を表わすラベルのラベル値として、暗号化しないパケットに対して割り当てるラベル値とは異なる値を使用し、両者のラベル値の相違により暗号化するパケットと暗号化しないパケットを区別するようにしたことを特徴とする請求項1記載のMPLSパケット処理方法。

【請求項4】 送信されるパケットは、レイヤ3パケットと複数のラベルスタックエントリからなるラベルスタックを含み、上記ノードがレイヤ3パケットを暗号化して送信する場合には、セキュリティアソシエーションに関する情報を表わすラベルスタックエントリに対しては上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオンにし、上記ノードがMPLSパケットを暗号化して送信する場合には、上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオフにすることを特徴とする請求項1又は3記載のMPLSパケット処理方法。

【請求項5】 上記セキュリティアソシエーションに関する情報を表わすラベルにおいて、そのラベル値に応じて異なる暗号処理プロセッサを用いて並列処理を行うようにしたことを特徴とする請求項1～4のいずれか1つに記載のMPLSパケット処理方法。

【請求項6】 上記暗号処理プロセッサは、上記ノードの外部に当該ノードとは別体で設けられていることを特徴とする請求項5記載のMPLSパケット処理方法。

【請求項7】 上記暗号化処理プロセッサを切り換えるために、上記暗号処理プロセッサと上記ノードとの間に設けられたスイッチをさらに有し、このスイッチは、ラベルスイッチと、イーサスイッチ等の通常のスイッチのいずれかであることを特徴とする請求項1～6のいずれか1つに記載のMPLSパケット処理方法。

【請求項8】 上記暗号化パケット処理は、パケットの暗号化と認証のうち少なくともどちらか一方を行うことを特徴とする請求項1～7のいずれか1つに記載のMP

L Sパケット処理方法。

【請求項9】 上記ノードは複数のVPNトンネルをサポートする暗号化パケット処理ノードであり、VPNトンネルがIPカプセル化のトンネルかMPLSのトンネルかに応じて適切なパケットフォーマットを選択するようにしたことを特徴とする請求項1～8のいずれか1つに記載のMPLSパケット処理方法。

【請求項10】 ラベルスイッチをサポートする2つのノードの間にラベルスイッチングパスが設定されており、2つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング(MPLS)のパケット処理装置であって、

パケットのセキュリティアソシエーションに関する情報を表すラベルをMPLSのラベルとして、暗号化されたレイヤ3パケットにカプセル化して送信する送信処理部と、

上記ラベルスイッチングパスを介して受信したパケットのセキュリティアソシエーションに関する情報に対応する暗号化方法を用いて受信パケットを復号する受信処理部と、

を具備することを特徴とするMPLSパケット処理装置。

【請求項11】 ラベルスイッチをサポートする2つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング(MPLS)のパケット処理方法であって、上記ラベルスイッチングパスの始点において、受信したレイヤ3パケットに、MPLSのラベルを含むパケットをカプセル化して転送することを特徴とするMPLSパケット処理方法。

【請求項12】 ラベルスイッチをサポートする2つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング(MPLS)のパケット処理装置であって、上記ラベルスイッチングパスの始点において、レイヤ3パケットに、MPLSのラベルを含むパケットをカプセル化して転送する転送処理部を有することを特徴とするMPLSパケット処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 MPLSパケット処理方法及びMPLSパケット処理装置に関するものである。

【0002】

【従来の技術】 近年インターネットを使い、企業ネットワークを構築するVPN (Virtual Private Network) が注目されている。特定のサイト間でのIPコネクティビティを、別のIPネットワーク(プロバイダネットワ

ーク)を用いて実現するVPN(Virtual Private Network)においては、コネクティビティを確保するサイト間でVPN内を流れるパケットをプロバイダネットワーク上に通すための「VPNトンネル」を生成する必要がある。このとき、サイトとプロバイダネットワークとの境界ルータがVPNトンネルのエンドポイントとなる。この境界ルータを「VPNエッジノード」とよぶ。VPNトンネル内を流れるIPパケットは、プロバイダネットワークを流れるIPパケットにカプセル化(IPカプセル化)されるか、あるいはMPLS(Multi-Protocol Label Switching)のLSP(Label Switched Path)を用いて実現される。一般に、プロバイダネットワークには、不特定多数のユーザがアクセス可能である。このため、VPNトンネルを流れるパケットの盗聴、改ざん等を防ぐためにVPNトンネルを流れるパケットに対して何らかのセキュリティ処理を施すことによりセキュアなVPN通信を確保する必要がある。セキュリティ処理には、暗号化と認証がある。

【0003】送信者が間違いなく本人であることを確認し他人による「なりすまし」を防止する認証機能や、通信データを暗号化して他人からのデータの盗み見やデータの改ざんを防止する暗号化機能をIPパケットに提供する技術として、IPSECがある。

【0004】図18にIPSECゲートウェイ(IPSEC-GW)によるIPSEC処理の仕組みを示す。そのメカニズムは以下の通りである。

【0005】1. 端末Aから端末B宛にIPパケットを送り出す。

【0006】2. IPSEC-GWはセキュリティ・ポリシー・データベース50とSAデータベース51を保持しており、入力された各パケットに対して、これらのデータベースを検索してIPSECの処理方法を調べる。まず、セキュリティ・ポリシーデータベース50を検索してIPSEC処理の有無を判定し、該当するSA(Security Association)を調べる。SAがない場合にはISAKMP(Internet Security Association and Key Management Protocol)を使用してSAを確立する。

【0007】3. 同様にしてSAデータベース51を検索する。SAデータベース51を検索すると当該SAに対応するIPSECの処理方法、例えばヘッダ種類、モード、アルゴリズムなどを調べることができる。

【0008】4. この後、IPSEC-GWは、IPSEC(暗号化されたIPパケット)を送り出す。すなわち、SAで指示された暗号化などの処理方法に従って暗号化などを実行してIPSECヘッダをつけてインターネット102にパケットを送り出す。

【0009】5. 受信側のIPSEC-GWはセキュリティ・ポリシー・データベース50'とSAデータベース51'を保持しており、入力された各パケットに対し

て、これらのデータベースを検索してIPSECの処理方法を調べる。ここではIPSECパケットを受信するとIPSECヘッダ中のSPI(Security Parameter Index)を調べる。

【0010】6. 次にSAデータベース51'を検索し、SPI値をもとに復号処理方法などを調べる。

【0011】7. IPSEC-GWはIPSEC処理を行った後、IPSECヘッダを取り除いて端末B宛にパケットを送信する。

【0012】図19に、IPSEC用のSA確立と鍵交換にかかわるISAKMP(Internet Security Association and Key Management Protocol)を示す。

【0013】1. ISAKMPフェーズの最初では、ISAKMPで使用するSA(ISAKMP-SA)をまず確立する。つまりこれから行うやり取りのためにお互いを認証しISAKMP用の鍵をやりとりする。

2. そしてISAKMPの次フェーズに移り、IPSECで使用するSA(IPSEC-SA)を確立する。

【0014】3. 鍵交換フェーズに入る。このフェーズではOaklayプロトコルを利用してIPSEC用の鍵を交換する。鍵交換にはOaklayプロトコルをISAKMPプロトコル上で使用する。ここでISAKMPの目的はIPSEC用のSAの確立と鍵交換にある。ISAKMPは鍵交換プロトコルでなく鍵交換プロトコルを利用するためのペイロードを提供している。実際の鍵交換はOaklayプロトコルを用いている。

【0015】図20はトランスポートモードとトンネルモードの各々における、IPパケット中のAHおよびESPヘッダ位置と、認証/暗号化範囲を示す図である。AH及びESPのSPIフィールドとシーケンス番号フィールドの位置は同じである。すなわち、1. トランスポートモードでは、オリジナルのIPヘッダの直後に位置し、2. トンネルモードではオリジナルのIPヘッダと新IPヘッダとの間に位置する。ESPのパディングデータや次ヘッダフィールド、認証データ用フィールドはパケットの後ろのフィールドに位置する。ESPの場合、暗号化範囲はいずれのモードでも同じで、シーケンス番号の直後から認証データの直前までであり、認証範囲はAHとESPとは異なっている。AHではIPヘッダの中の固定フィールドまで認証範囲とするのに対して、ESPではIPヘッダは認証範囲にしていない。

【0016】図21にAH(Authentication Header)の構造を示す。AHは送信者が間違いなく本人であることを認証するためのヘッダである。外部からのリプレイ攻撃を阻止するためにシーケンス番号が割り当ててある。なお、AHはIPパケットヘッダの直後に現れる。

【0017】図22にESP(Encapsulating Security Payload)の構造を示す。IPパケットまたはIPパケットからIPヘッダを除いたIPデータグラム部を暗号化してカプセル化し、ペイロード・データ部に埋め込

む。送信者が本人であることを認証する機能もある。

【0018】

【発明が解決しようとする課題】上記した方法でIPにカプセル化されたIPSECのパケットを処理(IP in IP)する場合、ルータはトンネルの入り口でL3フォワーディングテーブルのベストマッチ検索を2回行なう必要がある。つまり1回目は出口ルータを求めるために、2回目はその出口ルータへのNext Hopルータを求めるためである。したがって、このような検索処理によりルータの負荷が増大してしまうという問題があった。

【0019】一方、インターネット技術の標準化組織であるIETFで標準化されているMPLS(Multi-Protocol Label Switching)を用いることにより、VPN(Virtual Private Network)を構築することが可能である。しかしながら、VPNトンネルをMPLSで実現する場合に、セキュリティ処理のための具体的な機構が何ら考えられていなかった。したがって、1つのノードがIPカプセル化あるいは、MPLSのLSPで実現される複数のVPNをサポートする場合には、MPLSセキュリティ機能をサポートすることができなかった。

【0020】本発明はこのような課題に着目してなされたものであり、その目的とするところは、1つのノードがIPカプセル化あるいは、MPLSのLSPで実現される複数のVPNをサポートする場合でも、MPLSセキュリティ機能をサポートすることができるMPLSパケット処理方法及びMPLSパケット処理装置を提供することにある。

【0021】また、本発明の他の目的は、カプセル化ノードにおいて、宛先アドレスに関するベストマッチ検索を1回に減らすことができるMPLSパケット処理方法及びMPLSパケット処理装置を提供することにある。

【0022】

【課題を解決するための手段】上記の目的を達成するために、第1の発明は、ラベルスイッチをサポートする2つのノードの間にラベルスイッチングパスが設定されており、2つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング(MPLS)のパケット処理方法であって、パケットのセキュリティアソシエーションに関する情報を、MPLSのラベルとして用いてパケットの送信を行うようにする。

【0023】また、第2の発明は、第1の発明において、前記セキュリティアソシエーションに関する情報を表すラベルを含むパケットをレイヤ3パケットにカプセル化する。

【0024】また、第3の発明は、第1の発明において、上記セキュリティアソシエーションに関する情報を表すラベルのラベル値として、暗号化しないパケット

に対して割り当てるラベル値とは異なる値を使用し、両者のラベル値の相違により暗号化するパケットと暗号化しないパケットを区別する。

【0025】また、第4の発明は、第1または第3の発明において、送信されるパケットは、レイヤ3パケットと複数のラベルスタックエントリからなるラベルスタックを含み、上記ノードがレイヤ3パケットを暗号化して送信する場合には、セキュリティアソシエーションに関する情報を含むラベルスタックエントリに対しては上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオンにし、上記ノードがMPLSパケットを暗号化して送信する場合には、上記ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオフにする。

【0026】また、第5の発明は、第1～第4のいずれか1つの発明において、上記セキュリティアソシエーションに関する情報を表すラベルにおいて、そのラベル値に応じて異なる暗号処理プロセッサを用いて並列処理を行うようにする。

【0027】また、第6の発明は、第5の発明において、上記暗号処理プロセッサは、上記ノードの外部に当該ノードとは別体で設けられている。

【0028】また、第7の発明は、第1～第6のいずれか1つの発明において、上記暗号化処理プロセッサを切り換えるために、上記暗号化処理プロセッサと上記ノードとの間に設けられたスイッチをさらに有し、このスイッチは、ラベルスイッチと、イーサスイッチ等の通常のスイッチのいずれかである。

【0029】また、第8の発明は、第1～第7のいずれか1つの発明において、上記MPLSパケット処理は、パケットの暗号化と認証のうち少なくともどちらか一方を行う。

【0030】また、第9の発明は、第1～第8のいずれか1つの発明において、上記ノードは複数のVPNトンネルをサポートする暗号化パケット処理ノードであり、VPNトンネルがIPカプセル化のトンネルかMPLSのトンネルかに応じて適切なパケットフォーマットを選択する。

【0031】また、第10の発明は、ラベルスイッチをサポートする2つのノードの間にラベルスイッチングパスが設定されており、2つのノードの一方がパケットを暗号化して前記ラベルスイッチングパスを用いて暗号化パケットを送信し、他の一方が前記ラベルスイッチングパス上で受信した暗号化パケットを復号化するマルチプロトコルラベルスイッチング(MPLS)のパケット処理装置であって、パケットのセキュリティアソシエーションに関する情報を表すラベルをMPLSのラベルとして、暗号化されたレイヤ3パケットにカプセル化して送信する送信処理部と、上記ラベルスイッチングパスを介して受信したパケットのセキュリティアソシエーション

に関する情報に対応する暗号化方法を用いて受信パケットを復号する受信処理部とを具備する。

【0032】また、第11の発明は、ラベルスイッチをサポートする2つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング(MPLS)のパケット処理方法であって、上記ラベルスイッチングパスの始点において、受信したレイヤ3パケットに、MPLSのラベルを含むパケットをカプセル化して転送する。

【0033】また、第12の発明は、ラベルスイッチをサポートする2つのノードの間に設定されたラベルスイッチングパスを用いてパケットの転送を行うマルチプロトコルラベルスイッチング(MPLS)のパケット処理装置であって、上記ラベルスイッチングパスの始点において、レイヤ3パケットに、MPLSのラベルを含むパケットをカプセル化して転送する転送処理部を有する。

【0034】

【発明の実施の形態】まず、本発明の実施形態に係る暗号化パケット処理方法の概略を説明する。図1(a)はMPLSのフォーマットを示す図であり、L2ヘッダ100、シムヘッダ(Shimヘッダ)101、L3ヘッダ102、L4ヘッダ103、データ104からなる。

【0035】上記シムヘッダ101は、図1(b)に示すような、32ビットのラベルスタックエントリ(20ビットのラベル105、3ビットのエクスペリメンタルユース106、Sフラグ107、8ビットのTTL108からなる)を複数個並べたラベルスタックとなっている。ラベル105はパケット転送用またはSAラベルとして用いられ、これらのラベル値を異ならせることにより両者を区別できる。

【0036】また、複数個のラベルスタックエントリのうち、最後のエントリ以外のSフラグは0(オフ)となっており、最後のエントリのSフラグは1(オン)となっている。これによりラベルスタックの最後のエントリであるかどうかはSフラグの状態により判別することができる。L2ヘッダ100に隣接する第1のラベルスタックはパケット転送用のエントリである。本実施形態ではこのエントリと隣り合う第2のラベルスタックエントリのラベル105に上記したIPSECで用いたSPIに対応するSAラベル情報(例えば後述するLabel=s1)を挿入して送信する。

【0037】本実施形態では、IPカプセル化あるいは、MPLSのLSPで実現される複数のVPNトンネルをサポートするノードにおいて、パケットが転送されるVPNに対して以下の2つの適切な処理方式のいずれかを選択する手段を有する。

【0038】(第1の処理方式) IPカプセル化で実現される1つ以上のVPNトンネルをサポートするノードにおいて、パケットが転送されるVPNに対して以下の第1の処理方式を使用する手段を有する。すなわち、V

PNトンネルをIPカプセル化で実現し、必要に応じて、各VPNサイトで、パケットにMPLSラベルを付与した上で、レイヤ3(L3)のIPヘッダ(外部IPヘッダ)をつけてIP網を通過する機構を設ける。したがって、VPNトンネルを流れるパケットおよびMPLSラベルの情報は、L3パケットにカプセル化されている。通常のトンネルモードのIPsecと同様に内部IPヘッダも含めて暗号化を行う。また、暗号化されるパケットはIPパケットでなくてもよく、MPLSのShimヘッダがついたIPパケットであってもよい。つまり、外部IPヘッダをつけることによりVPNの出口までパケットが転送できる。SAを表すための情報として本処理方式では、SAを表す情報がエンコードされるラベル(SAラベル)を定義する。

【0039】VPNトンネルの入口側ルータでは、VPNトンネルにパケットを暗号化して送信する場合には、暗号化されたパケットに、SAラベル、LSP上のラベルスイッチングに使用されるラベル(トンネル出口ラベル)、の順にラベルスタックエントリをプッシュして送信する。SAラベルには、(セキュリティプロトコル、SPI)をマッピングさせる。

【0040】SAとSAラベルとのマッピングをVPNトンネルの両端のルータで行う必要があるが、この方法として、(i)両端のルータでマッピングを手動設定する方法と、(ii)ISAKMP(Internet Security Association and Key Management Protocol)などのプロトコルを用いて自動的に設定する方法の2種類がある。

【0041】暗号化されるパケットがIPパケットである場合には、SAラベルが入れられるラベルスタックエントリ中のラベルスタックの最後のエントリであることを示すフラグ(Sフラグ)をオンにする。

【0042】暗号化されるパケットがMPLSのラベル化パケットである場合には、SAラベルが入れられるラベルスタックエントリ中のSフラグをオフにする。

【0043】また、VPNトンネルを流れるパケットを暗号化しない場合には、SAラベルをつけないようにする。暗号化されないIPパケットがVPNトンネルを流れる場合には、トンネルの出口ラベルに対するラベルスタックエントリのSフラグがオンになる。暗号化されないMPLSのラベル化パケットがVPNトンネルを流れる場合には、トンネル出口ラベルに対するラベルスタックエントリのSフラグがオフになる。

【0044】このとき、次のラベルスタックエントリが存在するが、このラベルはSAラベルではない。したがって、トンネル出口ラベルの次のラベルとして、SAラベルがくる場合と、通常のラベルスイッチに使用されるラベル(パケット転送ラベル)がくる場合がある。そこでこれらを区別する必要があるため、SAラベルと、パケット転送ラベルとは異なるラベル値を割当てようとする。

【0045】VPNトンネルの出口側ルータでは、VPNトンネルからパケットを受信すると、外部IPヘッダを取り外し、先頭のトンネル出口ラベルをポップする。ポップした結果がIPパケットであれば、このIPパケットがセキュリティポリシー的に転送可能かどうかを判断し、転送可能であれば通常のIP転送を行い、転送が禁止されていれば直ちに廃棄する。

【0046】ポップした結果、次のラベルスタックエントリがあれば、もし、このエントリのラベルがSAラベルであるかどうかの判定を行う。もし、SAラベルでなくパケット転送ラベルであれば、ラベル値を元にセキュリティポリシー的に転送可能かどうかのチェックを行う。そして転送可能であれば、ラベルスイッチングによる転送を行い、転送が禁止されていれば、直ちに廃棄する。一方、SAラベルであれば、SAラベルをつけたまま受信パケットを暗号処理部に転送し、復号化処理を行う。

【0047】暗号処理部でパケットの復号化を行う場合には、SAラベル値にマッチするSAを決定し、マッチしたSAに対応する暗号化アルゴリズム、鍵情報を用いて復号化を行う。

【0048】復号化処理後、SAラベルが入っているラベルスタックエントリのSフラグがオフであれば、復号化したパケットをIPパケットとして転送し、Sフラグがオンであれば、復号化したパケットをMPLSのラベル化パケットとして転送する。

【0049】(第2の処理方式) 第2の処理方式ではVPNトンネルをMPLSのLSPで実現する。このときVPNトンネルを流れるパケットは、IPカプセル化の場合と同様に、内部IPヘッダも含めて暗号化が可能である。また、暗号化されるパケットはIPパケットでなくてもよく、MPLSのShimヘッダがついたIPパケットであってもよい。ただし、第1の処理方式(IPカプセル化)の場合と異なり、外部IPヘッダはつけないようにする。

【0050】外部IPヘッダをつけないため、SAを表すための情報が別に必要になる。そこで本処理方式では、SAを表す情報がエンコードされるラベル(SAラベル)を定義する。

【0051】VPNトンネルの入口側ルータでは、VPNトンネルにパケットを暗号化して送信する場合には、暗号化されたパケットに、SAラベル、LSP上のラベルスイッチングに使用されるラベル(トンネル出口ラベル)、の順にラベルスタックエントリをプッシュして送信する。

【0052】SAラベルには、(トンネル出口の宛先アドレス情報、セキュリティプロトコル、SPI)をマッピングさせる。また、トンネル出口ラベルをトンネル出口の宛先アドレス情報として使用する場合には、SAラベルには、(セキュリティプロトコル、SPI)をマッ

ピングさせ、トンネル出口ラベルとSAラベルの組によりSAを決定することも可能である。

【0053】SAとSAラベルとのマッピングをVPNトンネルの両端のルータで取る必要があるが、この方法として、(i)両端のルータでマッピングを手動設定する方法と、(ii)ISAKMP(Internet Security Association and Key Management Protocol)などのプロトコルを用いて自動的に設定する方法の2種類がある。

【0054】暗号化されるパケットがIPパケットである場合には、SAラベルが入れられるラベルスタックエントリ中のラベルスタックの最後のエントリであることを示すフラグ(Sフラグ)をオンにする。

【0055】暗号化されるパケットがMPLSのラベル化パケットである場合には、SAラベルが入れられるラベルスタックエントリ中のSフラグをオフにする。

【0056】また、VPNトンネルを流れるパケットを暗号化しない場合には、SAラベルをつけないようにする。暗号化されないIPパケットがVPNトンネルを流れる場合には、トンネルの出口ラベルに対するラベルスタックエントリのSフラグがオンになる。暗号化されないラベル化パケットがVPNトンネルを流れる場合には、トンネル出口ラベルに対するラベルスタックエントリのSフラグがオフになる。

【0057】このとき、次のラベルスタックエントリが存在するが、このラベルはSAラベルではない。したがって、トンネル出口ラベルの次のラベルとして、SAラベルがくる場合と、通常のラベルスイッチに使用されるラベル(パケット転送ラベル)がくる場合があり、これらを区別する必要がある。そこでここではSAラベルと、パケット転送ラベルとは異なるラベル値を割当てるようにする。

【0058】VPNトンネルの出口側ルータでは、VPNトンネルからパケットを受信すると、先頭のトンネル出口ラベルをポップする。ポップした結果が、IPパケットであれば、セキュリティポリシー的にこのIPパケットが転送可能であるかどうかを判断する。転送可能であれば通常のIP転送を行い、転送が禁止されていれば、直ちに廃棄する。

【0059】ポップした結果、次のラベルスタックエントリがあれば、もし、このエントリのラベルがSAラベルであるかどうかの判定を行う。もし、SAラベルでなくパケット転送ラベルであれば、ラベル値を元にセキュリティポリシー的に転送可能かどうかのチェックを行い、転送可能であれば、ラベルスイッチングによる転送を行い、転送が禁止されていれば、直ちに廃棄する。一方、もし、SAラベルであれば、SAラベルをつけたまま受信パケットを暗号処理部に転送し、復号化処理を行う。

【0060】暗号処理部でパケットの復号化を行う場合には、SAラベル値にマッチするSAを決定し、マッチ

したSAに対応する暗号化アルゴリズム、鍵情報を用いて復号化を行う。

【0061】復号化処理後、SAラベルが入っているラベルスタックエントリのSフラグがオフであれば、復号化した packets をIP packets として転送し、Sフラグがオンであれば、復号化した packets をMPLSのラベル化 packets として転送する。

【0062】なお、VPNエッジルータと暗号処理部は同じ機器にある必要はなく、別々の機器であってもよい。さらに、別々の機器の場合には、暗号処理部は、ネットワークインターフェースを持った暗号処理機器としてVPNエッジルータとネットワークを介して接続していてもよい。また、この場合には、暗号処理機器とVPNエッジルータの間の packets 転送をラベルスイッチにより実現してもよく、その際SAラベルを用いて packets をラベルスイッチしてもよい。

【0063】暗号処理部は、複数の暗号処理プロセッサから構成してもよい。VPNエッジルータは、SAラベルを参照して、複数の暗号処理プロセッサのいずれかに処理を振り分けることにより暗号処理の負荷分散を行ってもよい。ただし、負荷分散を行う場合には、 packets の順序逆転が起こらないように暗号化時に packets のヘッダ情報を参照して packets とSAのマッピングを決める必要がある。

【0064】以下、図面を参照して本発明の実施形態を詳細に説明する。

【0065】(第1実施形態)図2に、1つのノードがIPカプセル化(第1の処理方式)で1つ以上のVPNを構築する場合のネットワークの構成を示す。この図においては、E1-E2間のVPNを転送される packets はIPカプセル化され、宛先IPアドレスにより中継先が判定される。

【0066】図3に本実施形態の方式による暗号化処理を行うVPNの一例を示す。

【0067】図3において、E1, E2はVPNエッジルータ(暗号化ルータ)、R1, R2はVPNサイト内のラベルスイッチエッジルータ(R1, R2は異なるVPNサイトに属する)、SP1, SP2はセキュリティプロセッサ、SWはラベルスイッチである。本実施形態では、セキュリティプロセッサSP1, SP2と、VPNエッジルータE1, E2が別機器になっており、かつそれらはラベルスイッチSWにより接続されている場合を示す。P1, P2はR2が属するVPNサイト内に存在するネットワークアドレスプレフィクスである。

【0068】まず、R1が所属するVPNサイト内の図示されないホストから送信された宛先アドレスがP1にマッチする packets (L3-PDU) をR1が受信する(1)。

【0069】R1では、P1に対して出力ラベル=a11を割り当てているとすると、受信 packets に出力ラベ

ル=a11のラベルスタックエントリをプッシュしてE1に送信する。このとき、Sフラグはオンにする(2)。

【0070】E1はこの packets を受信する。E1では、入力ラベル=a11に対応して出力ラベルにラベルa12を割り当てており、さらに、 packets をSAラベル=s1を用いて暗号化するように設定されているとする。このときE1は、受信 packets に出力ラベル=a12のラベルスタックエントリをプッシュし、次にSAラベル=s1のラベルスタックエントリをプッシュしてラベルスイッチSWを経由してセキュリティプロセッサSP1に送る。

【0071】ラベルスイッチSWは、入力SAラベル=s1と、必要であれば packets のL2送信元アドレスも参照して packets のラベルスイッチングを行い、SP1に packets を転送する(2), (3)。

【0072】SP1はSAラベルs1をポップし、s1に対応するSAが使用する暗号化アルゴリズム、鍵を用いて packets を暗号化して、再びSAラベルs1をプッシュしてSW経由でE1に送信する(4)。このとき、暗号化される packets には、リプレイアタックを防ぐためのシーケンス番号(Seq. Num.)、および、認証のための情報(Auth.)を付加してもよい。

【0073】E1は、受信した packets のSAラベルを参照することによりトンネルの出口のVPNエッジルータE2を得る。E1において、E2に対するトンネル出口はE2であるため、E2のIPアドレスをIPヘッダの宛先IPアドレスに入れ、SAラベル=s1をL3-PDUにカプセルリングしてインターネット網13に送信する(5)。

【0074】インターネット13はこの packets を受信する。このとき、受信 packets のIPヘッダの宛先アドレスを見て中継処理が行われ、受信 packets はE2に送信される(6)。

【0075】E2はこの packets を受信すると、受信 packets のIPヘッダを見て、先頭のラベルスタックSAラベル=s1を参照して、ラベルスイッチSW経由でセキュリティプロセッサSP1に packets を送信する(7), (8)。

【0076】SP1はSAラベルs1をポップし、s1に対応するSAが使用する暗号化アルゴリズム、鍵を用いて packets を復号して、復号後の packets の先頭のラベルスタックエントリ中のラベル値=a13を参照してSW経由でE2に送信する(9)。

【0077】E2はこの packets を受信すると、受信 packets の先頭ラベルスタックエントリをポップする。ポップされたラベルスタックエントリ中の入力ラベル値a12には、出力ラベル値=a13が対応したとすると、E2は packets に出力ラベル値=a13が指定される packets ラベルスタックエントリをプッシュして、R2に

送信する(10)。

【0078】R2は受信パケットの先頭ラベルスタックエントリのLabel=a13をポップし、得られたIPパケットを通常のIP転送でサイト内の図示されない次段ルータに送信する(11)。

【0079】(第2実施形態)以下に本発明の第2実施形態を説明する。第2実施形態では、MPLSのLSPによりVPNトンネルを実現した場合の処理方式(第2の処理方式)を説明する。

【0080】図4にMPLSを用いた暗号化処理を行うVPNの一例を示す。

【0081】図4において、E1、E2はVPNエッジルータ(暗号化ルータ)、R1、R2はVPNサイト内のラベルスイッチエッジルータ(R1、R2は異なるVPNサイトに属する)、Aはプロバイダネットワーク内ルータ、SP1、SP2はセキュリティプロセッサ、SWはラベルスイッチである。本実施形態では、セキュリティプロセッサとVPNエッジルータが別機器になっており、かつそれらはラベルスイッチSWにより接続されている場合を示す。P1、P2はR2が属するVPNサイト内に存在するネットワークアドレスプレフィクスである。

【0082】まず、R1が所属するVPNサイト内の図示されないホストから送信された宛先アドレスがP1にマッチするパケットをR1が受信する(1)。

【0083】R1では、P1に対して出力ラベル=a11を割り当てているとすると、受信パケットに出力ラベル=a11のラベルスタックエントリをプッシュしてE1に送信する(2)。このとき、Sフラグはオンにする。

【0084】E1はこのパケットを受信する。E1では、入力ラベル=a11に対応して出力ラベルに対してラベルa12を割り当てており、さらに、パケットをSAラベル=s1を用いて暗号化するように設定されているとする。このときE1は、受信パケットに出力ラベル=a12のラベルスタックエントリをプッシュし、次にSAラベル=s1のラベルスタックエントリをプッシュしてラベルスイッチSWを経由してセキュリティプロセッサSP1に送る。

【0085】ラベルスイッチSWは、入力SAラベル=s1と、必要であればパケットのL2送信元アドレスも参照してパケットのラベルスイッチングを行い、SP1にパケットを転送する(2)、(3)。

【0086】SP1はSAラベルs1をポップし、s1に対応するSAが使用する暗号化アルゴリズム、鍵を用いてパケットを暗号化して、再びSAラベルs1をプッシュしてSW経由でE1に送信する(4)。このとき、暗号化されるパケットには、リプレイアタックを防ぐためのシーケンス番号(Seq. Num.)、および、認証のための情報(Auth.)を付加してもよい。

【0087】E1は、受信したパケットのSAラベルを参照することによりトンネルの出口のVPNエッジルータE2を決める。E1において、E2に対するトンネル出口ラベル=b1とすると、E1は受信パケットに出力ラベル=b1のラベルスタックエントリをプッシュしてプロバイダネットワークAに送信する(5)。

【0088】Aはこのパケットを受信する。このとき、受信パケットの入力ラベル=b1に対して出力ラベル=b2を割り当てているとすると、Aは受信パケットの入力ラベルスタックエントリをラベル=a11のラベルスタックエントリにスワップしてE2に送信する(6)。

【0089】E2はこのパケットを受信すると、受信パケットの先頭のラベルスタックエントリをポップする。次に、SAラベル=s1を参照して、ラベルスイッチSW経由でセキュリティプロセッサSP1にパケットを送信する(7)、(8)。

【0090】SP1はSAラベルs1をポップし、s1に対応するSAが使用する暗号化アルゴリズム、鍵を用いてパケットを復号して、復号後のパケットの先頭のラベルスタックエントリ中のラベル値=a13を参照してSW経由でE1に送信する(9)。

【0091】E2はこのパケットを受信すると、受信パケットの先頭ラベルスタックエントリをポップする。ポップされたラベルスタックエントリ中の入力ラベル値a12には、出力ラベル値=a13が対応したとすると、E2はパケットに出力ラベル値=a13が指定されるパケットラベルスタックエントリをプッシュして、R2に送信する(10)。

【0092】R2は受信パケットの先頭ラベルスタックエントリをポップし、得られたIPパケットを通常のIP転送でサイト内の図示されない次段ルータに送信する(11)。

【0093】(第3実施形態)以下に本発明の第3実施形態を説明する。図5に上記したIPネットワークとMPLSネットワークが混在し、1つのノードがIPカプセル化及び、MPLSのLSPでVPNを構築する場合のネットワークの構成を示す。図5においては、E1-E2間のVPNを転送されるパケットはIPカプセル化され、宛先IPアドレスにより中継先が判定されている。また、E1-E3間のVPNを転送されるパケットはMPLSラベルが付加され、MPLSラベルにより中継先が判定されている。

【0094】E1においては、IPカプセル化によるVPNとMPLSのLSPによるVPNをサポートする必要がある。したがってE1ではまず初めにパケットが転送されるVPNトンネルにより、上記の2つの処理方式のいずれかを選択する。

【0095】図6は、この2つの処理方式のいずれかを選択する工程を示すフローチャートである。VPNトンネルの送信側のノードにおいては、受信したパケットの

宛先アドレスと当該パケットが転送されるVPNがIPカプセル化により実現されるのか、MPLSのLSPにより実現されるのかを対応づけるテーブルを用意し、このテーブルを参照することですずれの処理方式を選択する。

【0096】一方、VPNトンネルの受信側のノードにおいては、図5のようなIP、MPLS混在のネットワーク構成において、ポート毎にVPNトンネルの種類が異なっているのであれば、受信パケットが到着したポートとそのポートがサポートするVPNの種類を予め対応づけておけば良い。

【0097】ステップS1の判断により受信パケットが転送されるVPNトンネルがMPLSかどうかを判断し、MPLSである場合にはステップS2のパケット受信処理（MPLSラベル化パケット）を行い、MPLSでない場合にはステップS3のパケット受信処理（IPパケット）を行う。各受信処理の詳細は上記した通りである。

【0098】（第4実施形態）以下に本発明の第4実施形態を説明する。図7に本実施形態を用いたVPNエッジルータが、IPパケットを受信した場合の処理を説明するためのフローチャートを示す。

【0099】受信パケットヘッダをH、H中のプロトコル番号をPr、H中の宛先アドレスをDとする（ステップS10）。次のステップS11でDが自ノードアドレスの一つと一致するかどうかを判断し、もし、Dが自ノードアドレスの一つと一致していなければ、後述する暗号側処理1（ステップS14）を行う。Dが自ノードアドレスの一つと一致している場合には次のステップS12でPrがESPまたはAHであるかどうかを判断し、もし、PrがESPまたはAHのいずれでもなければ後述する暗号側処理1（ステップS14）を行い、PrがESPまたはAHのいずれかであれば、後述する復号側処理1（ステップS13）を行う。

【0100】図8に本実施形態のVPNエッジルータが、MPLSのラベル化パケットを受信した場合の処理を説明するためのフローチャートを示す。

【0101】まずステップS20で、受信パケットの先頭ラベルスタックエントリのラベル値をLiとし、このLiに対応するVPN内のパケット転送に使用される出力ラベル（トンネル外出力ラベル）をLoとする。

【0102】次のステップS21では、先頭のラベルスタックエントリをポップし、ポップしたラベルスタックエントリ中のラベル値をs1とし、ポップ後のパケットをPとする。次のステップS22においてLo=Nullかどうかを判断し、もし、LoがNullでなければ、後述する暗号側処理2（ステップS26）を行い処理を終了する。もし、LoがNullであれば、ステップS23でs1=Nullかどうかを判断し、s1がNullでなければ後述する復号側処理2（ステップS2

5）を行って処理を終了し、s1がNullであればPはIPパケットであるため、ステップS24でPを通常のIP転送により次段ルータに送信して処理を終了する（次段ルータが自ルータであればPのIPヘッダを取り除いて所定の上位レイヤアプリケーションに渡す）。

【0103】図9に暗号側処理1の詳細を説明するためのフローチャートを示す。

【0104】まず、受信パケットのペイロードをPとし（ステップS30）、次のステップS31で受信パケットの宛先アドレスDに対するトンネル出口ルータのアドレスをE2、E2への次段ルータに対する出力インターフェースアドレスをE1とする。次にステップS32で受信パケットのヘッダHにベストマッチするセクタをSとし、このSに対するセキュリティポリシーをPoとする。

【0105】次のステップS34でPoにて示されるセキュリティポリシーが非暗号化、廃棄、暗号化のどれであるかを判断し、セキュリティポリシーが非暗号化であれば、P' := Pとし（ステップS35）、P'を宛先アドレスE2、送信元アドレスE1のIPパケットにカプセル化して送信し（ステップS39）、処理を終了する。

【0106】一方、ステップS34の判断においてセキュリティポリシーが廃棄であれば、Pを直ちに廃棄して処理を終了する（ステップS33）。一方、Poにて示されるセキュリティポリシーが暗号化であれば、ステップS36でSに対するセキュリティプロトコルをPrとするとともに、A := (S, E2, Pr)とし、次のステップS37でAが使用するSPIをIとする。次にステップS38で、Pを、Aに対する暗号化アルゴリズムおよび鍵を用いて暗号化し、暗号化されたパケットをP'とし、次のステップS39でP'を宛先アドレスE2、送信元アドレスE1のIPパケットにカプセル化して送信し、処理を終了する。

【0107】図10に復号側処理1の詳細を説明するためのフローチャートを示す。まずステップS40で、受信パケットのペイロードをPとし、受信パケットの宛先アドレスDに対するトンネル出口ルータのアドレスをE2、Pに対するセキュリティプロトコルをPrとする。次のステップS41では、Pに対するSPIをI、A := (I, E2, Pr)、Iが使用するセキュリティプロセッサ（SP）の番号をMとする。

【0108】次にステップS42で、PをAに対する復号化アルゴリズムおよび鍵を用いて番号MのSPで復号化し、復号化されたパケットをP'とする。次のステップS43で復号化に成功したかどうかを判断し、もし、復号化に失敗すれば、直ちにP'を廃棄（ステップS46）して処理を終了する。そうでなければ、以下の処理を行う。

【0109】すなわち、ステップS44に進んでIに対

するセキュリティデータベースのセクタをSとする。また、P' にベストマッチするセクタをS' とする。さらに、Sに対するセキュリティポリシーをPoとする。

【0110】次にステップS45に進んでSとS' が一致し、かつPoが暗号化であるかどうかを判断し、もし、SとS' が一致しないかまたはPoが暗号化でない場合には、直ちにP' を廃棄（ステップS46）して処理を終了する。そうでない場合には、P' を次段ルータに送信（ステップS47）して処理を終了する。

【0111】図11に、暗号側処理2の詳細を説明するためのフローチャートを示す。

【0112】まずステップS50で、入力側ラベルLiに対するトンネル出口ルータのアドレスをE2とし、次のステップS51でLiにベストマッチするセキュリティデータベースのセクタをSとするとともに、Sに対するセキュリティポリシーをPoとする。次にステップS53でPoにて示されるセキュリティポリシーが非暗号化、廃棄、暗号化のどれであるかを判断し、セキュリティポリシーが非暗号化であれば、P' := Pとし（ステップS54）、ステップS59に移行してP' にs1をプッシュして宛先アドレスE2のIPパケットにカプセル化して送信し、処理を終了する。

【0113】一方、ステップS53においてPoにて示されるセキュリティポリシーが廃棄であれば、Pを直ちに廃棄（ステップS52）して処理を終了する。一方、ステップS53においてPoにて示されるセキュリティポリシーが暗号化であれば、ステップS55でSに対するセキュリティプロトコルをPrとし、A := (S, E2, Pr)とし、次のステップS56でAが使用するSPIラベルをs1とする。

【0114】次に、Pの先頭のラベルスタックエントリのラベル値をLoとし（ステップS57）、次のステップS58でPをAに対する暗号化アルゴリズムおよび鍵を用いて暗号化し、暗号化されたパケットをP' とする。次にステップS59でP' にs1をプッシュして、宛先アドレスE2、送信元アドレスE1のIPパケットにカプセル化して送信し、処理を終了する。

【0115】図12に復号側処理2の詳細を説明するためのフローチャートを示す。

【0116】まずステップS60で、ラベル値s1に対するプロトコルIDをPrとする。次にステップS61で、Prがセキュリティプロトコルを表わしているかどうかを判断し、Noであれば以下を実行する。

【0117】P' := Pとし（ステップS66）、P' にベストマッチするセキュリティデータベースのセクタをS、Sに対するセキュリティポリシーをPoとする（ステップS67）。次にステップS68でPoが非暗号化であるかどうかを判断し、Poが非暗号化でなければ、直ちにP' を廃棄（ステップS71）して処理を終

了する。そうでなければステップS69に進んで、s1がラベルスタックの最後のエントリのラベルであるかどうかをチェックする。ここでYESであればステップS73に進んで、P' を通常のIP転送により次段ルータに送信し（次段ルータが自ルータであればPのIPヘッダを取り除いて所定の上位レイヤアプリケーションに渡す）、そうでなければ、ステップS2に進んでLiをLoに書き換え、P' をLoに対する次段ルータに送信して処理を終了する。

【0118】一方、ステップS61においてPrがセキュリティプロトコルを表していれば、ステップS62に進んでPをs1に対する復号化アルゴリズムおよび鍵を用いて復号化し、復号化されたパケットをP' とする。

【0119】ステップS63で復号化に成功したかどうかを判断し、復号化に失敗すれば、直ちにP' を廃棄（ステップS71）して処理を終了する。そうでなければ、ステップS64に進んで、s1に対するセキュリティデータベースのセクタをSとする。また、P' にベストマッチするセクタをS' とする。また、Sに対するセキュリティポリシーをPoとする。

【0120】次にステップS65に進んで、S=S' かつPoが暗号化であるかどうかを判断し、もし、SとS' が一致しないかまたはPoが暗号化でない場合には、直ちにP' を廃棄（ステップS1）して処理を終了する。そうでない場合にはステップS69に進んで、s1がラベルスタックの最後のエントリのラベルであるかどうかをチェックし、そうであればステップS73に進んで、P' を通常のIP転送により次段ルータに送信する（次段ルータが自ルータであればPのIPヘッダを取り除いて所定の上位レイヤアプリケーションに渡す）。また、最後のエントリのラベルでなければ、ステップS70に進んでP' の先頭ラベルをLiにして、Liに対するトンネル外出力ラベルをLoにする。次のステップS72で、LiをLoに書き換え、P' をLoに対する次段ルータに送信して処理を終了する。

【0121】図13に本実施形態で用いられるセキュリティデータベースの構成を示す。

【0122】図13においては、トンネル出口のVPNエッジルータがE2であるようなVPNトンネルを用いて転送されないパケットは廃棄される。

【0123】また、トンネル出口のVPNエッジルータがE2であるようなパケットのうち、パケットの送信元アドレスがH11であるようなパケットは、セキュリティプロトコルESP、暗号化アルゴリズムA1、鍵K1を用いて暗号化され、パケットの送信元アドレスがH12であるようなパケットは、セキュリティプロトコルE2、暗号化アルゴリズムA2、鍵K2を用いて暗号化され、パケットの送信元アドレスがH11, H12以外のパケットはそのまま送信される。

【0124】図14に本実施形態におけるVPNトンネ

ル上を転送されるパケットのパケットフォーマットを示す。

【0125】図14において、トンネルPDU (IPv4) はVPNトンネル上を転送されるIPv4パケットを含むレイヤ2ヘッダ以下のPDUであり、トンネルPDU (IPv6) はVPNトンネル上を転送されるIPv6パケットを含むレイヤ2ヘッダ以下のPDUである。また、[A]はAが省略可能であることを示し、{A||B}はA、Bのいずれか1つを選択することを示す。{A||B||C}はA、B、Cのいずれか1つを選択することを示す。

【0126】図15に、図7から図12に示すフローチャートの処理を実現するノードのブロック図を示す。

【0127】ノードは、パケット入力部201、IP/MPLSヘッダ解析部202、自ノード宛パケット処理部200、暗号処理部206、復号処理部203、セキュリティデータベース (SD) 204、暗号化側セキュリティポリシー決定部205、IP/MPLSパケットフォワーディング処理部208、パケット出力部209、復号化側セキュリティポリシー決定部207から構成される。

【0128】ノードは、パケット入力部201からパケットを受信すると、IP/MPLSヘッダ解析部202にて、パケットのL2ヘッダの情報を用いて、受信パケットがIPパケットかMPLSのラベル化パケットかを決定し、それぞれのパケットに依存したヘッダ処理を行う。

【0129】もし、受信パケットが自ノード宛のパケットであれば以下のいずれかが実行される。すなわち、ヘッダ情報からペイロードがセキュリティ処理されていることが判明すれば、復号処理部203にて復号処理を行う。そうでなければ、自ノード宛パケット処理部200にて上位レイヤ処理を行う。

【0130】復号処理部203では、SD204を検索し、MPLSのSAラベル値にマッチするエントリがあれば、そのエントリに対して使用される暗号化アルゴリズム、鍵を用いて、ペイロードの復号化処理を行う。次に、復号化側セキュリティポリシー決定部207において、復号化後により得られるIPパケットヘッダまたはMPLSヘッダと、SD204の内容とからパケットをフォワード可能かどうかを決定し、可能であれば、IP/MPLSパケットフォワーディング処理部208にて出力インターフェースを決め、パケット出力部209からIPパケットまたはMPLSパケットを出力する。

【0131】一方、受信パケットが自ノード宛のパケットでなければ、暗号化側セキュリティポリシーにて、SD204の検索を行う。もし、受信ヘッダ情報にマッチするようなSDエントリがなければパケットを廃棄する。一方、そのようなSDエントリがある場合には以下のいずれかの処理を行う。

【0132】すなわち、パケットを暗号化する必要がなければ、IP/MPLSフォワーディング処理部208にてIPヘッダまたはMPLSヘッダの情報から出力インターフェースを決め、パケット出力部209からパケットを出力する。一方、パケットを暗号化する必要がある場合は、暗号処理部206において、受信パケットにマッチしたSD204のエントリにて指定される暗号化アルゴリズム鍵を用いてパケットの暗号化を行う。その際、IP/MPLSフォワーディング処理部208にてIPヘッダまたはMPLSヘッダの情報から出力インターフェースを決め、パケット出力部209からパケットを出力する。

【0133】(第5実施形態) 以下に本発明の第5実施形態を説明する。図16に本実施形態で用いられる暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノード内に配置した場合のハード構成の一例を示す。

【0134】図16において、暗号処理ノードは、スイッチ部300、ネットワークインターフェース部301、内部処理インターフェース部303および、中央処理部 (CPU+Mem) 302から構成される。なお、スイッチ部300を用いるかわりに、内部バスを用いることにより、スイッチ部、ネットワークインターフェース部、内部処理インターフェース部および、中央処理部間のデータ転送を実現してもよい。

【0135】各ネットワークインターフェース部301はセキュリティデータベース (SD) およびフォワーディングテーブル (FW) を持つ。また、各内部処理インターフェース部303は、セキュリティプロセッサ部 (SP) およびフォワーディングテーブル (FW) を持つ。中央処理部302は、自ノード宛のIPパケットのうちペイロードがIPのPDUでないもの (IP-in-IPでないもの) に対する処理および、FW, SD, SPの管理を行う。

【0136】ノードは、パケットをネットワークインターフェース部301から受信した場合には、まず、受信パケットのIPヘッダまたはMPLSヘッダの情報からパケットが自ノード宛かどうかを調べ、一致しない場合には、以下の処理を行う。

【0137】まず、ネットワークインターフェース部301内のフォワーディングテーブル (FW) を参照してトンネル出口を決定する。次に、セキュリティデータベース (SD) を参照し、パケットに対してセキュリティ処理を行わない場合には、スイッチ部経由でトンネル出口に対する出力インターフェースにパケットを出力する。パケットに対して暗号化処理を行う場合には、SAラベル、および処理すべき内部処理インターフェース部303を決定した後、パケットにトンネル出口ラベル、SAラベル (暗号化の必要がなければNullが指定される)、の順にプッシュした後、これをスイッチ部30

0を通して決定した内部処理インターフェース部303に送信する。

【0138】内部処理インターフェース部303では、まず、SAラベルをポップする。次に、ポップ後のパケットの先頭にあるトンネル出口ラベルをキーに内部処理インターフェース部303内のFWを参照して、指定されたトンネル出口に対する出力ネットワークインターフェース部を決定する。次に、SAラベルがNullでなければパケットをSPで暗号化処理後、スイッチ部300を通して出力ネットワークインターフェース部に送信する。出力ネットワークインターフェースは、スイッチ部300から出力されたパケットを、パケットの先頭にあるトンネル出口ラベルを用いて、ラベルスイッチングする。

【0139】一方、ノードがパケットをネットワークインターフェース部301から受信した場合に、パケットが自ノード宛である場合には、以下の処理を行う。

【0140】まず、ペイロードが上位プロトコルレイヤパケットであれば、パケットを中央処理部302に送信し、そうでなければ、セキュリティデータベース(SD)を参照し、SA情報および処理すべき内部処理インターフェース部303を決定した後、受信パケットのペイロード、SAラベル値(受信パケットがSAラベルを持たなければNULL値となる)を、スイッチ部300を通して決定した内部処理インターフェース部303に送信する。内部処理インターフェース部303では、必要であればペイロードをSPで復号化処理後、復号化後のペイロード(=暗号化前のPDU)の先頭部に存在する暗号化前のパケットヘッダの情報またはMPLSヘッダの情報を元に内部処理インターフェース部303内のFWを参照して、指定された宛先アドレスに対する出力ネットワークインターフェース部を決定し、スイッチ部300を通して出力ネットワークインターフェース部に送信する。出力ネットワークインターフェースは、スイッチ部300から出力された復号化後のペイロード(=暗号化前のPDU)、レイヤ2処理を行った後、これを外部に出力する。

【0141】(第6実施形態)以下に本発明の第6実施形態を説明する。図17に本実施形態で用いられる暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノードとネットワーク的に接続する装置として配置した場合のハード構成の一例を示す。

【0142】図17において、暗号処理ノードは、スイッチ部400、ネットワークインターフェース部401、および、中央処理部(CPU+Mem)402から構成される。なお、スイッチ部400を用いるかわりに、内部バスを用いることにより、スイッチ部、ネットワークインターフェース部、内部処理インターフェース部および、中間処理部間のデータ転送を実現してもよい。また、暗号処理ノードは、セキュリティ処理インタ

ーフェース403を介して、イーサネット404上にイーサスイッチ405を介して接続するセキュリティプロセッサ(SP)406に接続される。

【0143】イーサスイッチ405は、ラベルスイッチング機能を持っていてもよい。このとき、ノードからセキュリティプロセッサ(SP)406に送られるパケットは、MPLSヘッダをもち、かつ、そのパケットが含まれるイーサネットフレームの宛先アドレスは、イーサスイッチ405のMACアドレスとなる。

【0144】各ネットワークインターフェース部401はセキュリティデータベース(SD)およびフォワーディングテーブル(FW)を持つ。中央処理部402は、自ノード宛のIPパケットのうちペイロードがIPのPDUでないもの(IP-in-IPでないもの)に対する処理および、FW、SD、SPの管理を行う。

【0145】ノードは、パケットをネットワークインターフェース部401から受信した場合には、まず、受信パケットのIPヘッダまたはMPLSヘッダの情報からパケットが自ノード宛かどうかを調べ、一致しない場合には、以下の処理を行う。

【0146】まず、ネットワークインターフェース部401内のFWを参照してトンネル出口を決定する。次に、セキュリティデータベース(SD)を参照し、パケットに対してセキュリティ処理を行わない場合には、スイッチ部400経由でトンネル出口に対する出力インターフェースにパケットを出力する。パケットに対して暗号化処理を行う場合には、SA、および処理すべきセキュリティプロセッサ(SP)406を決定した後、トンネル出口用ラベルスタックエントリ、SA用ラベルスタックエントリの順にパケットのペイロードにプッシュして、これをスイッチ部400を通してセキュリティ処理インターフェース403に送信する。セキュリティ処理インターフェース403は、SA用ラベルスタックエントリを参照して、イーサスイッチ405経由で所定のセキュリティプロセッサ(SP)406にパケットをイーサネット(登録商標)フレーム化して送信する。

【0147】イーサスイッチ405は、ラベルスイッチング機能を有する場合でかつ、自ノード宛のMPLSヘッダ付きのパケットを受信すると、先頭のラベルスタックエントリを参照して所定のセキュリティプロセッサ(SP)406にパケットをフォワードする。ラベルスイッチング機能を有しない場合には、単に通常のイーサスイッチとして動作する。

【0148】セキュリティプロセッサ(SP)406では、パケットの先頭のラベルスタックをポップし、ポップしたラベルスタックエントリ中のSAラベル値を参照してパケットを暗号化処理後、SAラベル値を参照して暗号化後のパケットをノードに返す。ノードは、このパケットの先頭のラベルスタックエントリを参照して、トンネル出口ノードに対してパケットを送信する。

【0149】一方、ノードがパケットをネットワークインターフェース部401から受信した場合に、パケットが自ノード宛である場合には、以下の処理を行う。

【0150】まず、先頭のラベルスタックをポップする。結果として得られたパケットが上位プロトコルレイヤパケットであれば、パケットを中央処理部402に送信し、そうでなければ、セキュリティデータベース(SD)を参照し、SA情報および処理すべきセキュリティプロセッサ(SP)406を決定した後、次のラベルスタックエントリを参照する。エントリ中のラベルがSAラベルでなければ、このラベル値をもとに通常のラベルスイッチングによりパケットを転送する。SAラベルであれば、パケットを、スイッチ部400を通してセキュリティ処理インターフェース403に送信する。セキュリティ処理インターフェース403は、SA用ラベルスタックエントリを参照して、イーサスイッチ405経由で所定のセキュリティプロセッサ(SP)406にパケットをイーサネットフレーム化して送信する。

【0151】イーサスイッチ405は、ラベルスイッチング機能を有する場合でかつ、自ノード宛のMPLSヘッダ付きのパケットを受信すると、先頭のラベルスタックエントリを参照して所定のセキュリティプロセッサ(SP)406にパケットをフォワードする。ラベルスイッチング機能を有しない場合には、単に通常のイーサスイッチとして動作する。

【0152】セキュリティプロセッサ(SP)406では、パケットの先頭のラベルスタックエントリをポップし、この情報を元にペイロードを復号化処理後、復号化後のペイロード(=暗号化前のPDU)をノードに返す。ノードは、受信したパケットがIPヘッダを持てばパケットをIP転送し、MPLSヘッダを持てばパケットをラベルスイッチングする。

【0153】以上、上記した実施形態によれば、1つのノードがIPカプセル化あるいは、MPLSのLSPで実現される複数のVPNをサポートする場合でも、MPLSセキュリティ機能をサポートすることができる。

【0154】また、トンネルの入り口でMPLSのラベルを含むパケットをレイヤ3パケットにカプセル化しているので、単なるIPカプセル化の場合に比べてカプセル化ノードにおいて、宛先アドレスに関するベストマッチ検索の回数を2回から1回に減らすことができる。

【0155】レイヤ3テーブルを2回検索する必要がなくなり、検索によるルータの付加を軽減できる。

【0156】また、セキュリティ処理が必要であることを示すSAラベルと、セキュリティ処理が必要でないラベルの値が重複しないようにしたので、暗号化パケットと非暗号化パケットの識別が可能となる。

【0157】また、ノードがレイヤ3パケットを暗号化して送信する場合には、セキュリティアソシエーションに関する情報を含むラベルスタックエントリに対しては

ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオンにし、ノードがMPLSパケットを暗号化して送信する場合には、ラベルスタックの最後のラベルスタックエントリであることを示すフラグをオフにする。これによって、MPLSパケットとレイヤ3パケットの両方を暗号化してMPLSパケットとしてVPNトンネル上でラベルスイッチングすることが可能になる。

【0158】また、SAラベル値を参照して、ラベル値が異なるパケットは異なる暗号処理プロセッサで並列処理を行うようにしたので、トラヒックの負荷が高い場合に並列処理を行わない場合に比べて暗号処理の高速化が可能となる。

【0159】さらに、暗号処理プロセッサは暗号化パケット処理ノード内に存在せず、ネットワーク的に暗号化パケット処理ノードと接続することが可能となるため、スケーラブルかつフレキシブルな暗号処理ノードの構成が可能となる。

【0160】また、復号側ノードでは、パケットを暗号処理するかどうかの判定、暗号処理する場合には使用されるセキュリティアソシエーションの決定、暗号処理しない場合にはどのノードにパケットをフォワードするか等の決定、がすべてラベル値を参照することにより行われるため、パケット処理の一元化および高速化が可能となる。

【0161】

【発明の効果】請求項1～10に記載の発明によれば、1つのノードがIPカプセル化あるいは、MPLSのLSPで実現される複数のVPNをサポートする場合でも、MPLSセキュリティ機能をサポートすることができ

【0162】また、請求項3に記載の発明によれば、セキュリティ処理が必要であることを示すSAラベルの値と、セキュリティ処理が必要でないラベルの値が重複しないようにしたので、暗号化パケットと非暗号化パケットの識別が可能となる。

【0163】また、請求項4に記載の発明によれば、MPLSパケットとレイヤ3パケットの両方を暗号化してMPLSパケットとしてVPNトンネル上でラベルスイッチングすることが可能になる。

【0164】また、請求項5に記載の発明によれば、SAラベル値を参照して、ラベル値が異なるパケットは異なる暗号処理プロセッサで並列処理を行うようにしたので、トラヒックの負荷が高い場合に並列処理を行わない場合に比べて暗号処理の高速化が可能となる。

【0165】また、請求項6に記載の発明によれば、ネットワーク的に暗号化パケット処理ノードと接続することが可能になるため、スケーラブルかつフレキシブルな暗号処理ノードの構成が可能となる。

【0166】また、請求項11及び12に記載の発明に

よれば、カプセル化ノードにおいて、宛先アドレスに関するベストマッチ検索の回数を2回から1回に減らすことができる。

【図面の簡単な説明】

【図1】1つのノードがIPカプセル化で1つ以上のVPNを構築する場合のネットワークの構成を示す図である。

【図2】IPカプセル化による暗号化処理を行うVPNの一例を示す図である。

【図3】MPLSのフォーマットを示す図である。

【図4】MPLSを用いた暗号化処理を行うVPNの一例を示す図である。

【図5】IPネットワークとMPLSネットワークとが混在した場合のネットワーク構成を示す図である。

【図6】IP、MPLS処理方式のいずれかを選択する工程を示すフローチャートである。

【図7】VPNエッジルータが、IPパケットを受信した場合の処理を説明するためのフローチャートである。

【図8】本実施形態のVPNエッジルータが、MPLSのラベル化パケットを受信した場合の処理を説明するためのフローチャートである。

【図9】暗号側処理1の詳細を説明するためのフローチャートである。

【図10】復号側処理1の詳細を説明するためのフローチャートである。

【図11】暗号側処理2の詳細を説明するためのフローチャートである。

【図12】復号側処理2の詳細を説明するためのフローチャートである。

【図13】本実施形態で用いられるセキュリティデータベースの構成を示す図である。

【図14】本実施形態におけるVPNトンネル上を転送されるパケットのパケットフォーマットを示す図である。

【図15】図7から図12に示すフローチャートの処理を実現するノードのブロック図である。

【図16】本実施形態で用いられる暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノード内に配置した場合のハード構成の一例を示す図である。

【図17】本実施形態で用いられる暗号処理ノードの構

成として、並列処理を行うセキュリティプロセッサをノードとネットワーク的に接続する装置として配置した場合のハード構成の一例を示す図である。

【図18】IPSECゲートウェイ(IPSEC-GW)によるIPSEC処理の仕組みを示す図である。

【図19】IPSEC用のSA確立と鍵交換にかかわるISAKMP(Internet Security Association and Key Management Protocol)を示す図である。

【図20】トランスポートモードとトンネルモードの各々における、IPパケット中のAHおよびESPヘッダ位置と、認証/暗号化範囲を示す図である。

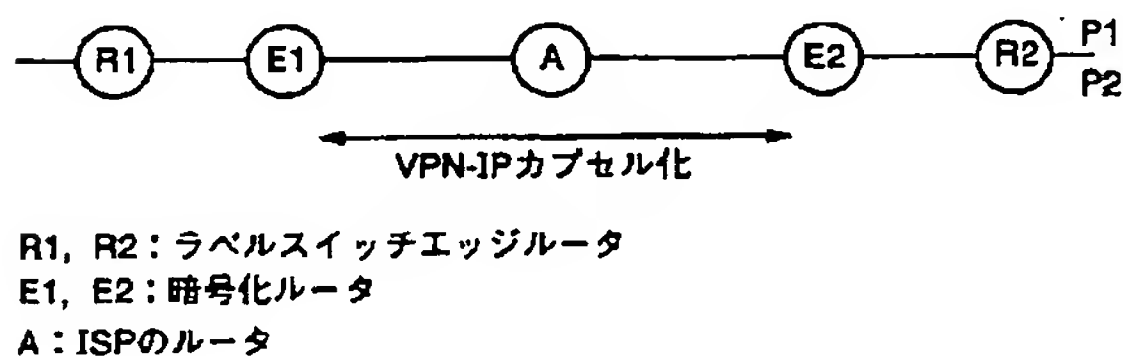
【図21】AH(Authentication Header)の構造を示す図である。

【図22】ESP(Encapsulating Security Payload)の構造を示す図である。

【符号の説明】

E1、E2…VPNエッジルータ(暗号化ルータ)、
R1、R2…ラベルスイッチエッジルータ、
SP1、SP2…セキュリティプロセッサ、
SW…ラベルスイッチ、
100…L2ヘッダ、
101…シムヘッダ、
102…L3ヘッダ、
103…L4ヘッダ、
104…データ、
105…ラベル、
106…エクスペリメンタルユースビット、
107…Sフラグ、
108…TTLビット
200…自ノード宛パケット処理部、
201…パケット入力部、
202…IP/MPLSヘッダ解析部、
203…復号処理部、
204…セキュリティデータベース(SD)、
205…暗号化側セキュリティポリシー決定部、
206…暗号処理部、
207…復号化側セキュリティポリシー決定部、
208…IP/MPLSパケットフォワーディング処理部、
209…パケット出力部。

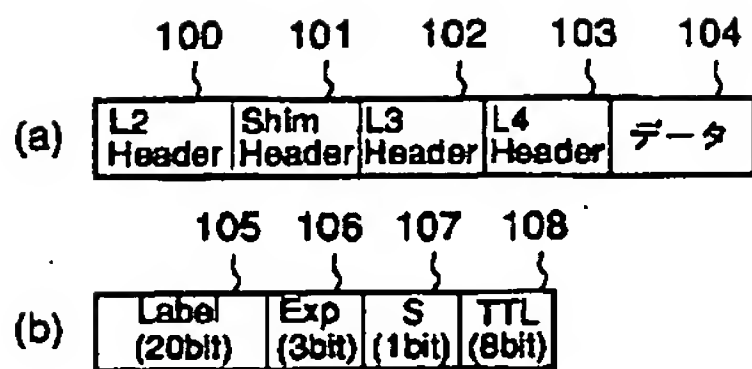
【図2】



【図13】

トンネル出口	セクタ	ポリシー	SPI	セキュリティマーク/アルゴリズム/鍵
				アルゴリズム/鍵
	送信元アドレス=H11	暗号化	100	ESP/A1/K1
E2	送信元アドレス=H12	暗号化	200	ESP/A2/K2
	その他	非暗号化		
その他	指定なし	廃棄		

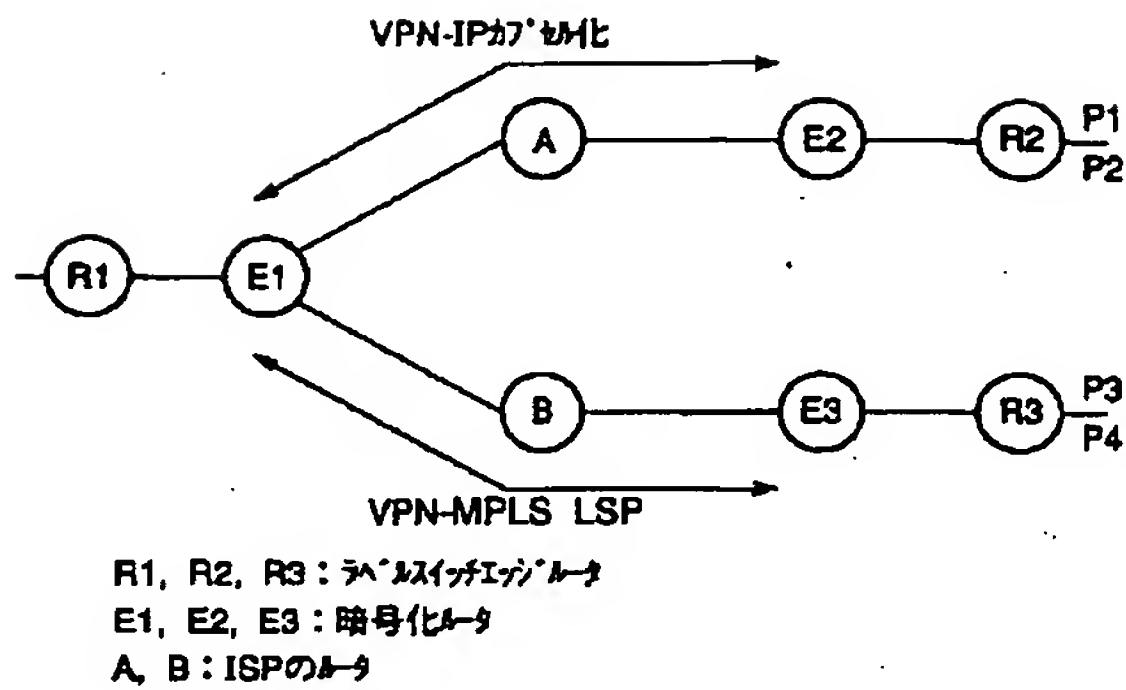
【図1】



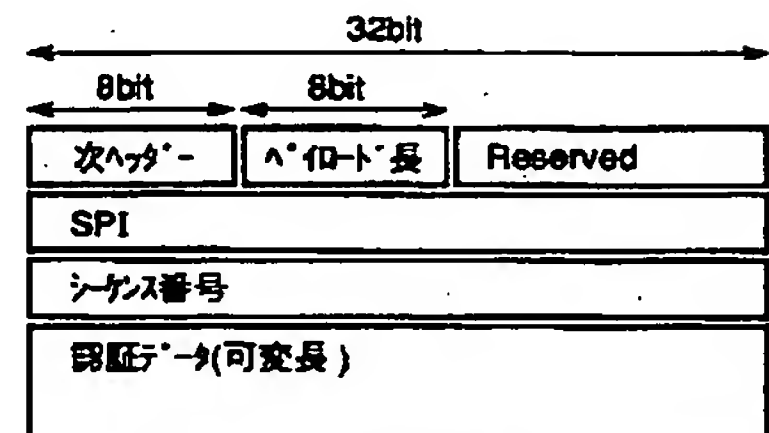
Label: Label Value, 20bits
Exp: Experimental Use, 3bits
S: Bottom of Stack, 1bit
TTL: Time to Live, 8bits

1. Label Value
2. Experimental Use
Experimental Useであり、未定義
3. Bottom of Stack (S)
Label Stackの最後のEntry(Bottom Label Stack)の場合、
"1"を設定する
Bottom Label Stackでなければ、"0"を設定する
4. Time to Live (TTL)
TTLをEncodeする

【図5】

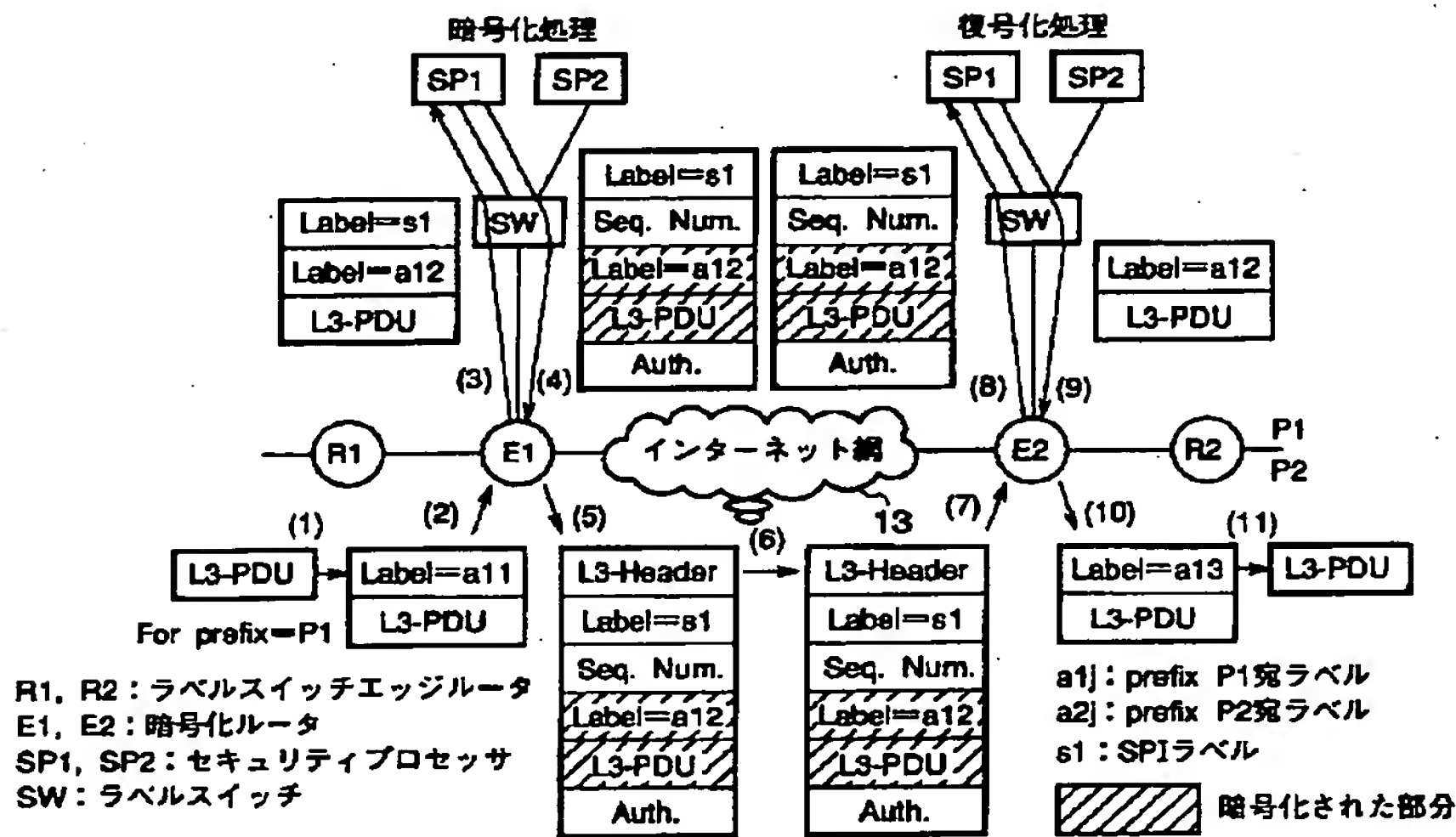


【図21】

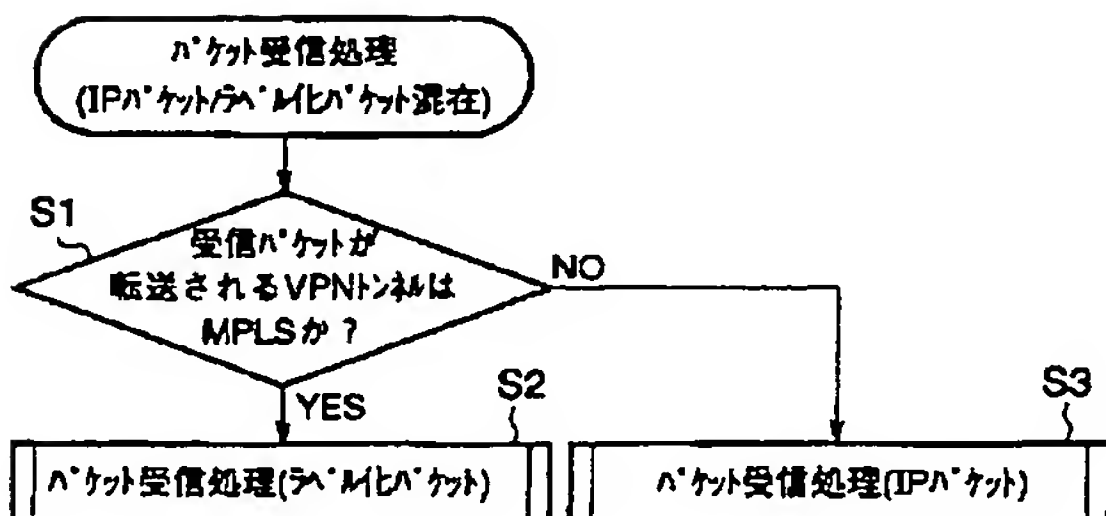


- ・次ヘッダー: 認証データの次に来る7バイト番号
- ・シーケンス番号: リプレイ攻撃を防止するため、
各パケットに順序番号を付ける

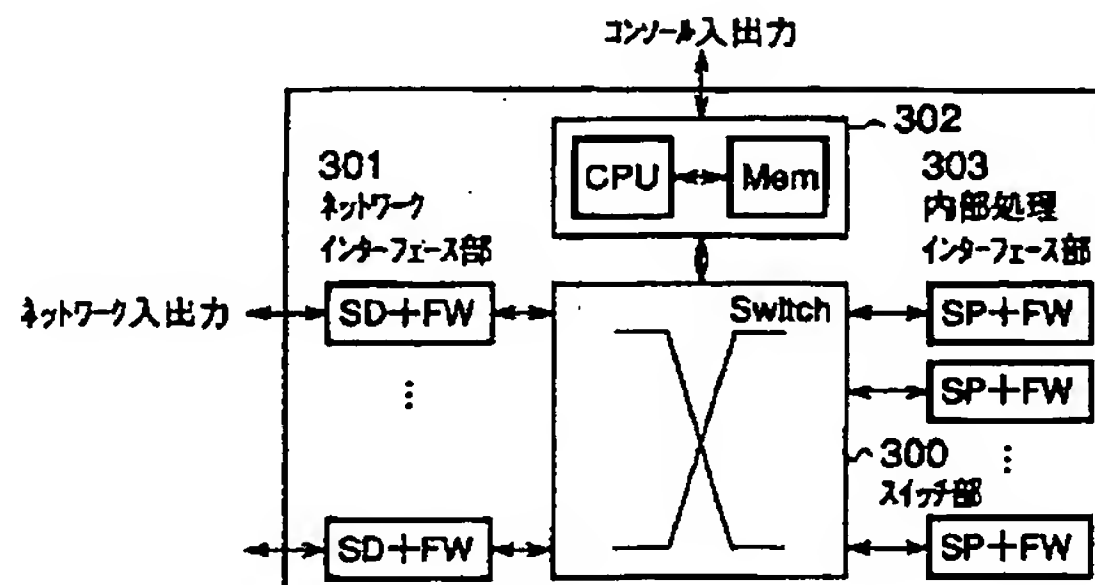
【図3】



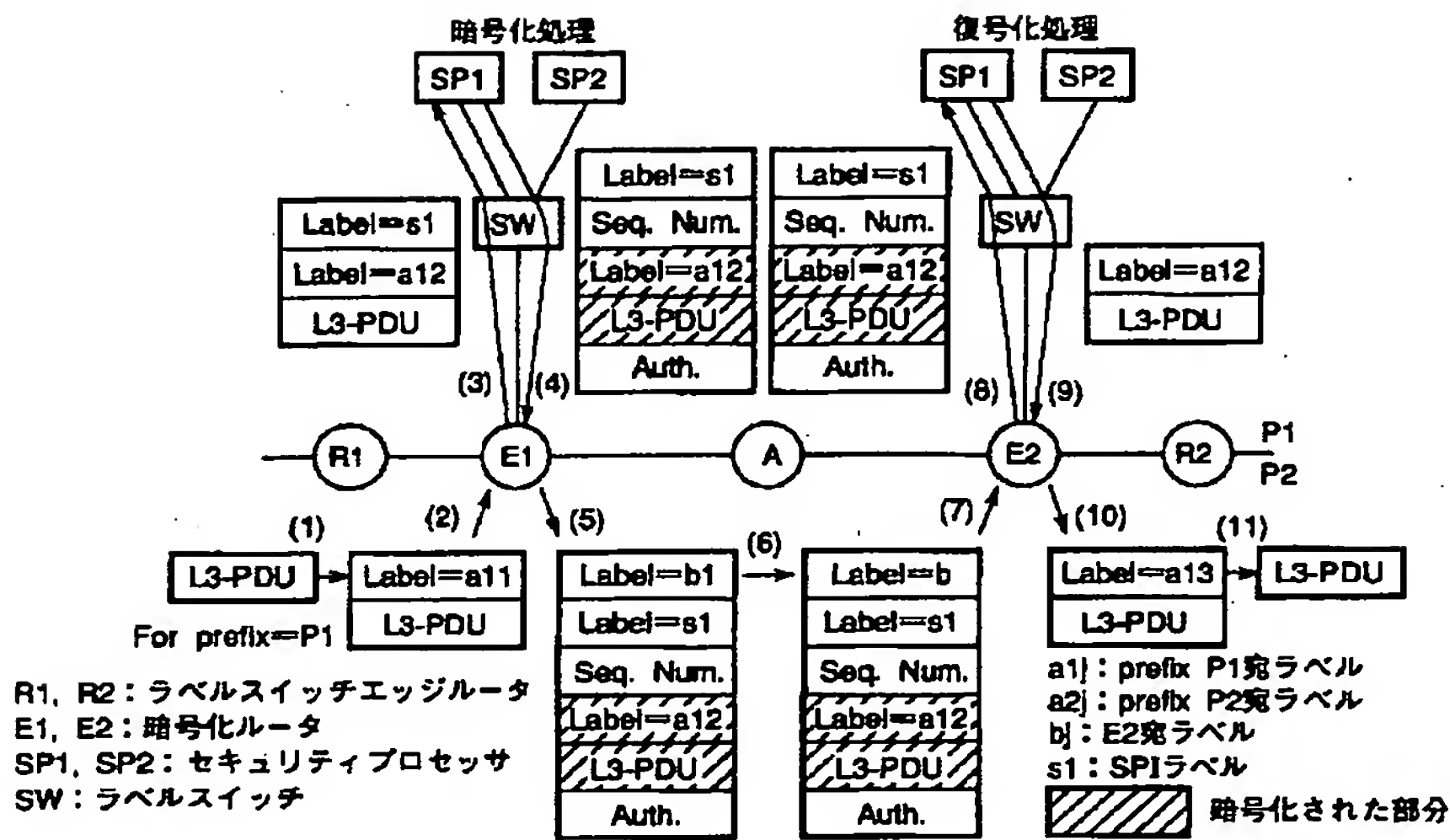
【図6】



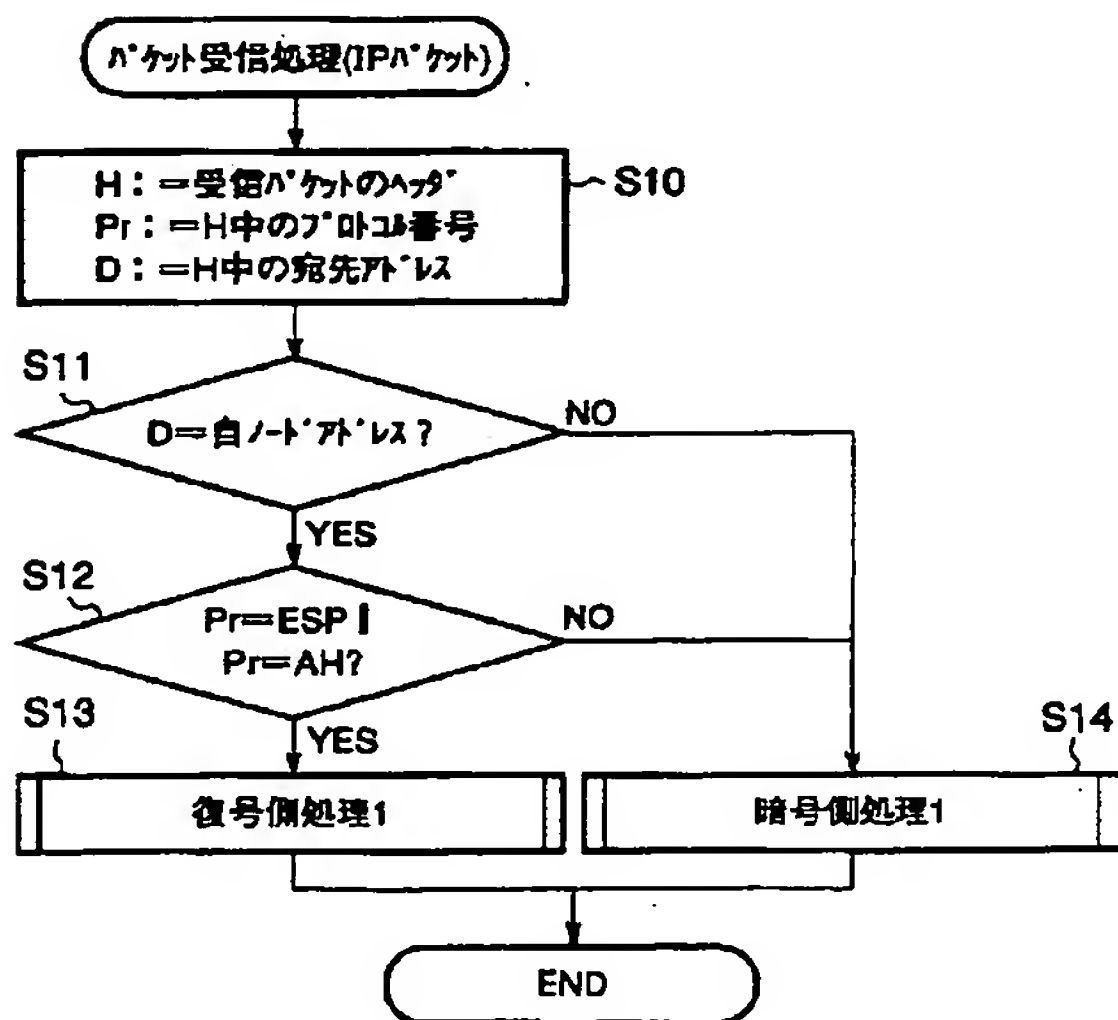
【図16】



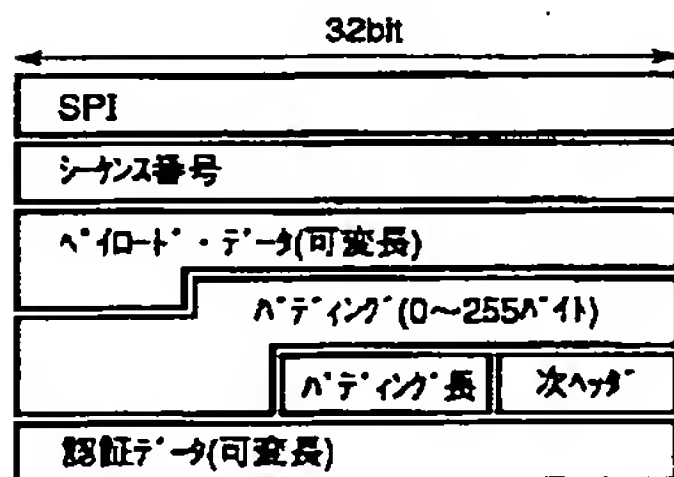
【図4】



【図7】

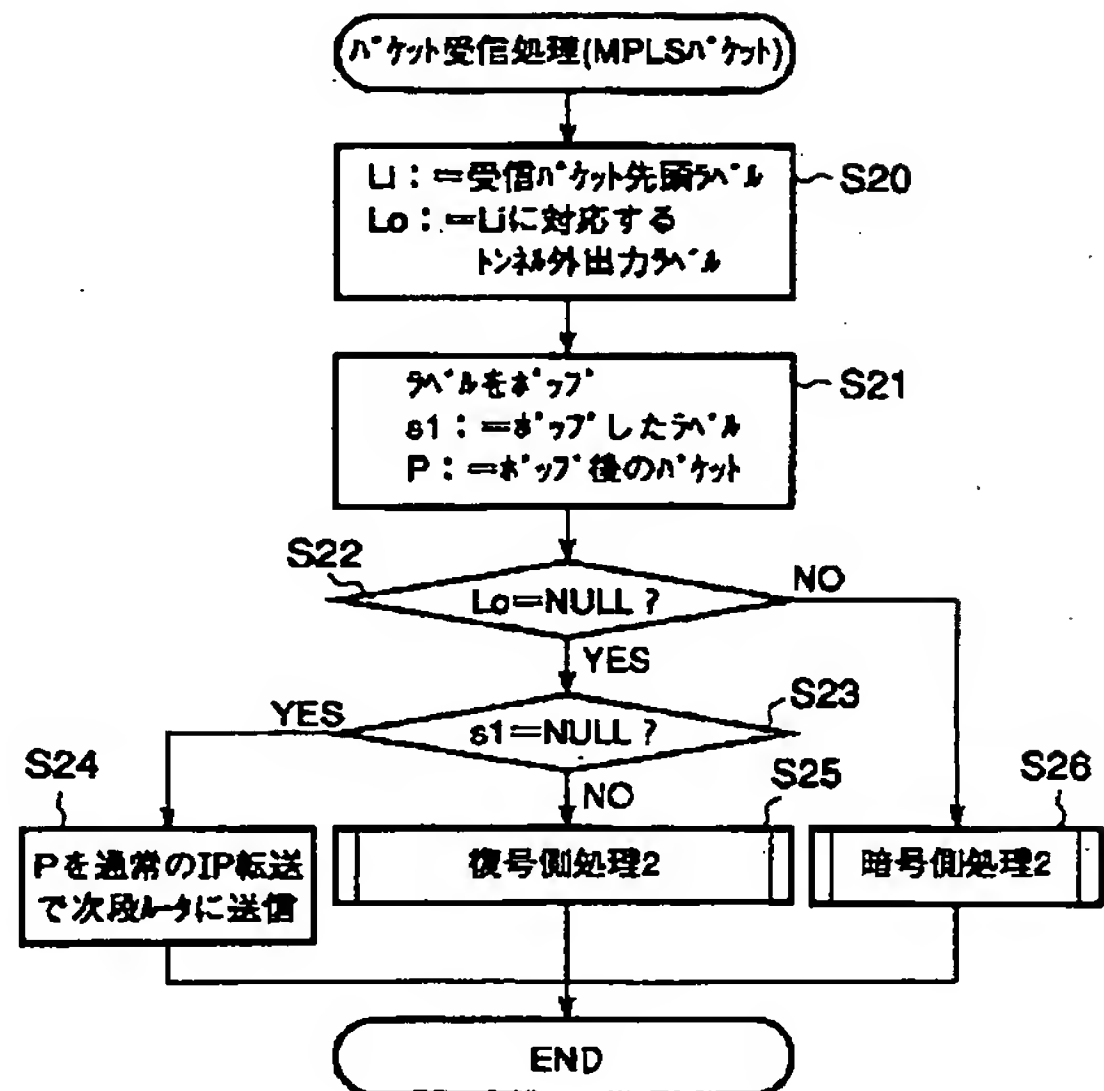


【図22】

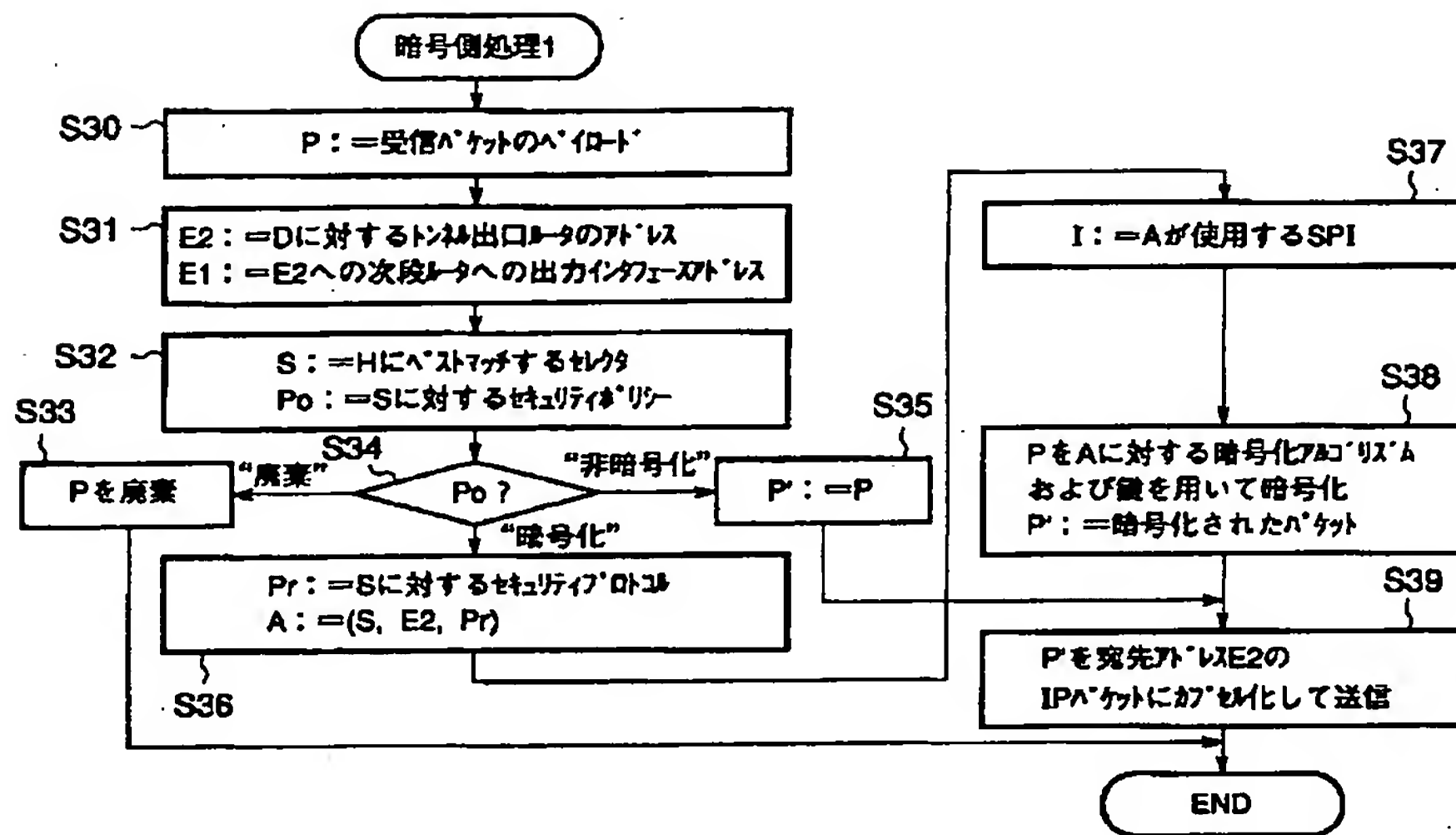


- ・ SPI: SPI値と宛先IPアドレスで該当するSAを一意に指定する
- ・ シーケンス番号: リプレイ攻撃を阻止するために順序番号を付ける
- ・ ヘッディング: パケット長を調整するためのヘッディング・データ
- ・ 認証データ: ESPヘッダ、暗号鍵、ヘッダをハッシュ化したデータ

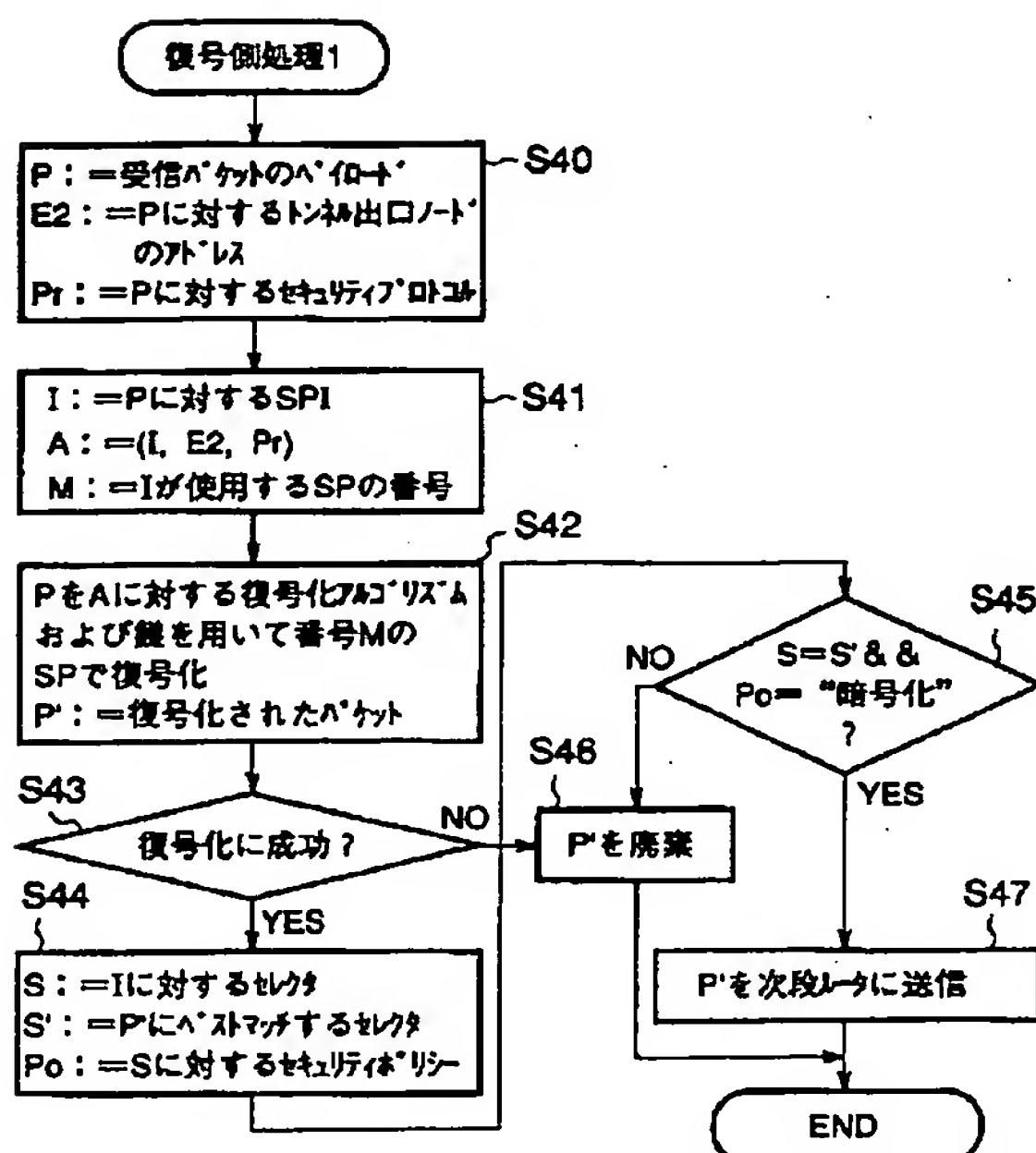
【図8】



【図9】



【図10】



【図14】

トンネルPDU(IPv4) := ヘッダ + [LSE + ...] + LSE +
[ESP || SPIなしESP || IPv4パケット]
トンネルPDU(IPv6) := ヘッダ + [LSE + ...] + LSE +
[ESP [+IPv6拡張ヘッダ] || SPIなしESP
[+IPv6拡張ヘッダ] || IPv6パケット]

LSE := ラベル(20bits) + Exp(3bits) + S(1bits) + TTL(8bits)

SPIなしESP := シーケンス番号(4octets) + ヘッダフィールド(可変長) +
パディング(0~255octets) + パディング長(1octet) +
次ヘッダ(1octet) + 認証データ(可変長)

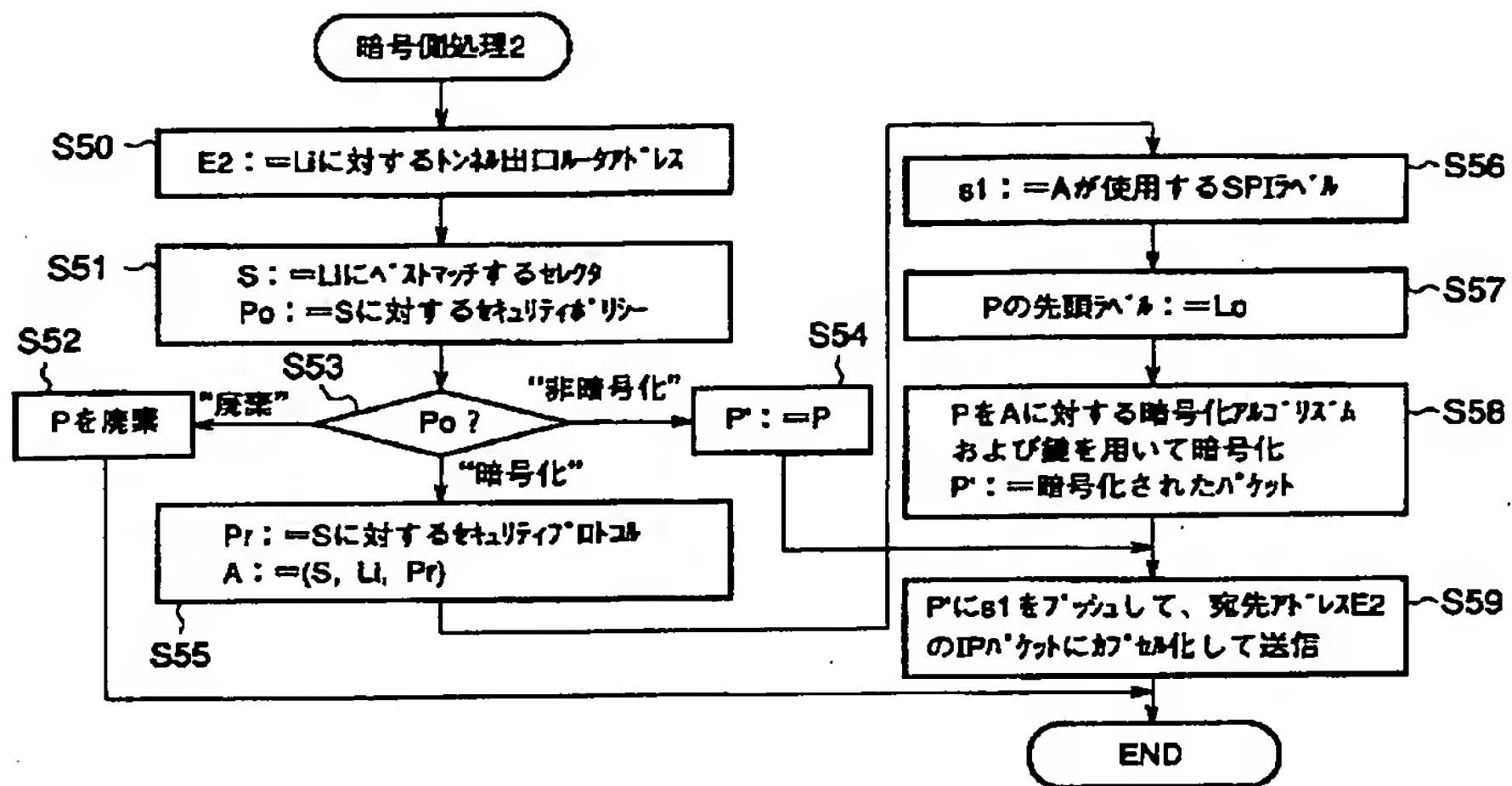
ESP := SPI + SPIなしESP

ヘッダフィールド := Encrypt(暗号化前ヘッダフィールド)

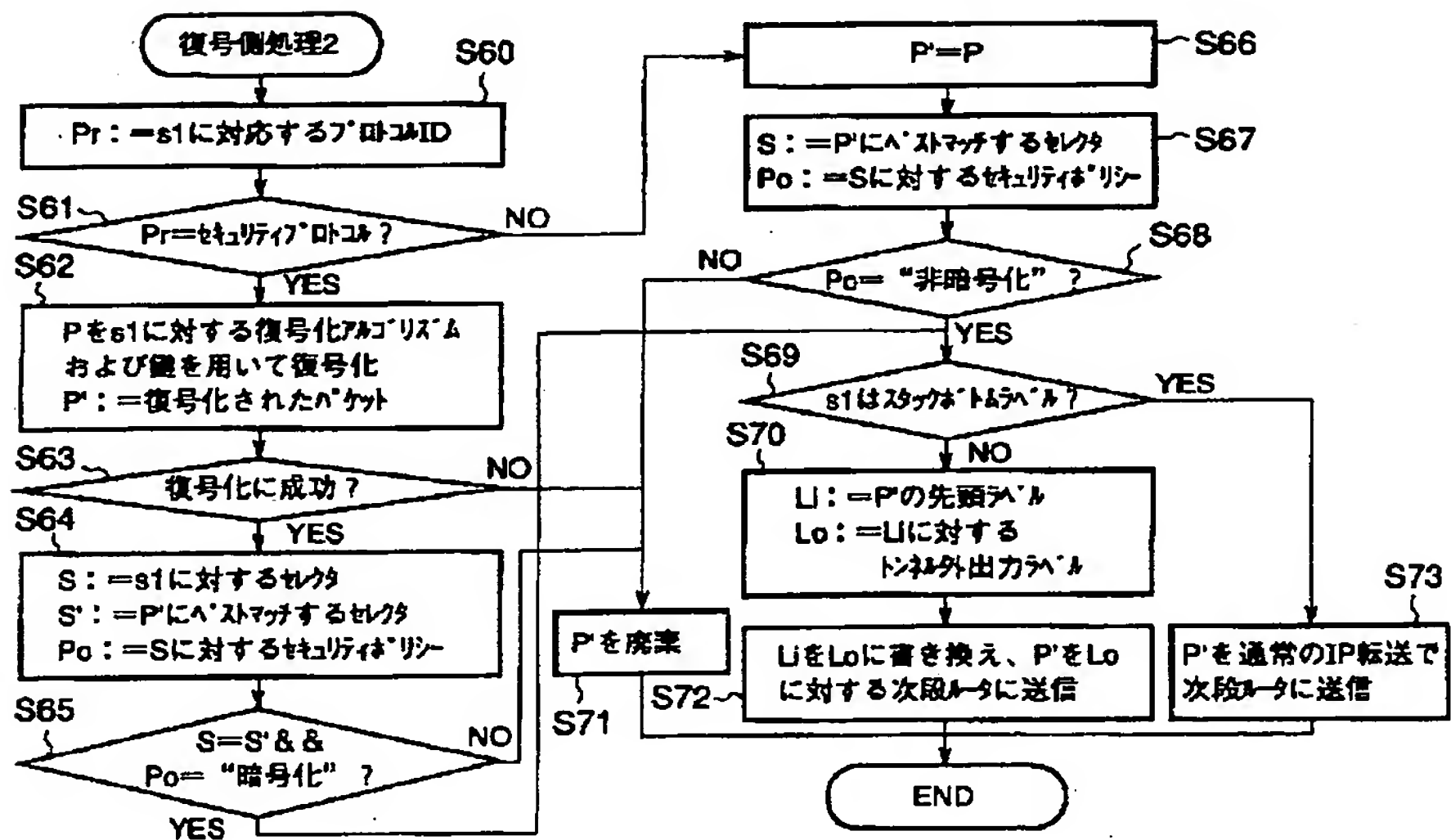
暗号化前ヘッダ := {IPパケット || [LSE + ...] + LSE + IPパケット}

LSE : Label Stack Entry
ESP : Encapsulating Security Payload
SPI : Security Parameter Index
Exp : Experimental Field
TTL : Time To Live

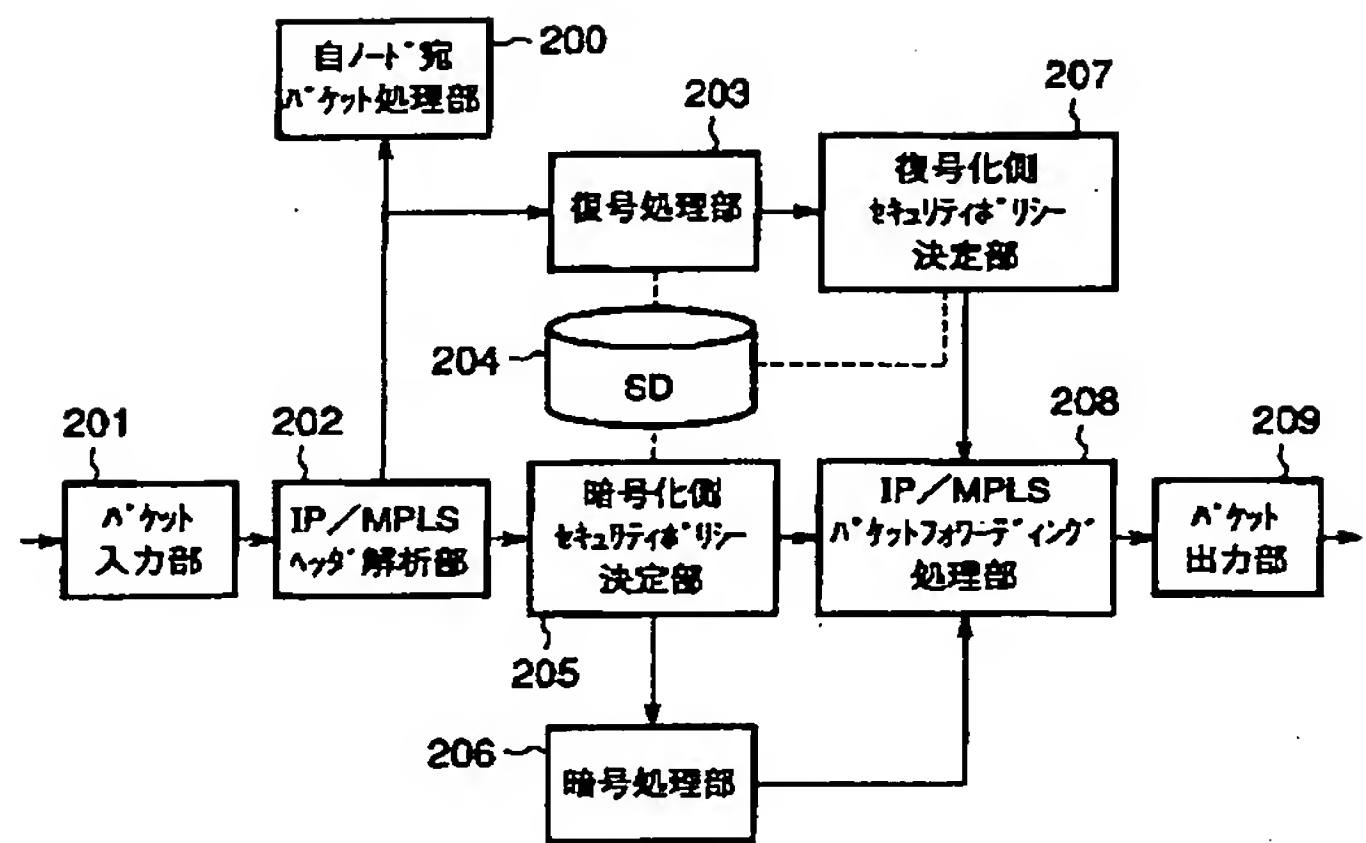
【図11】



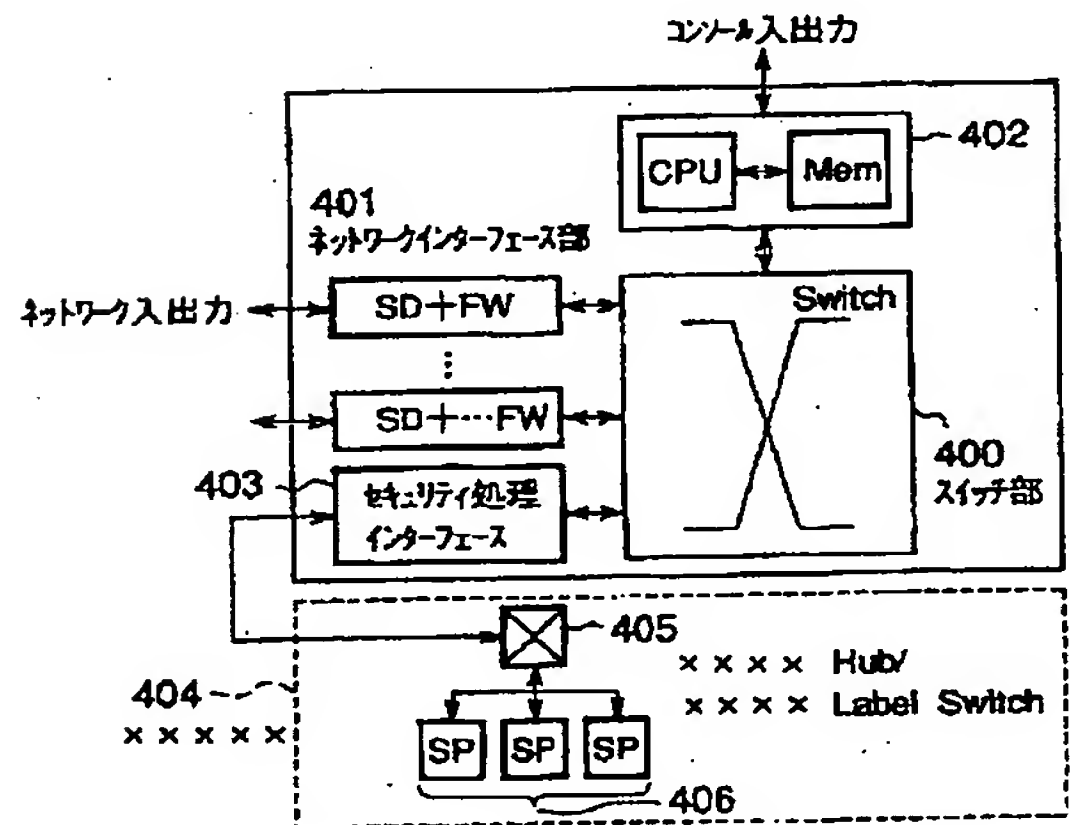
【図12】



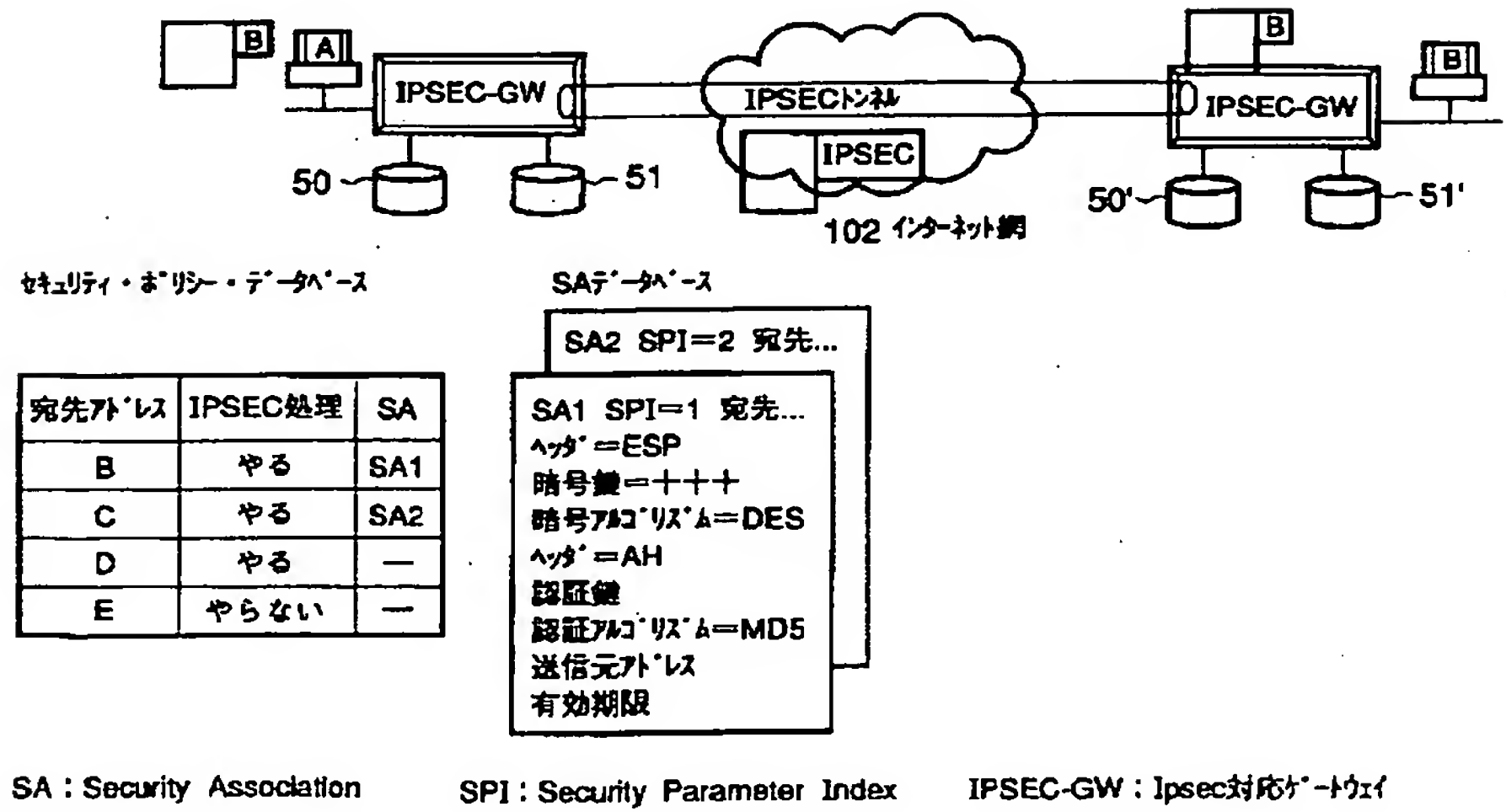
【図15】



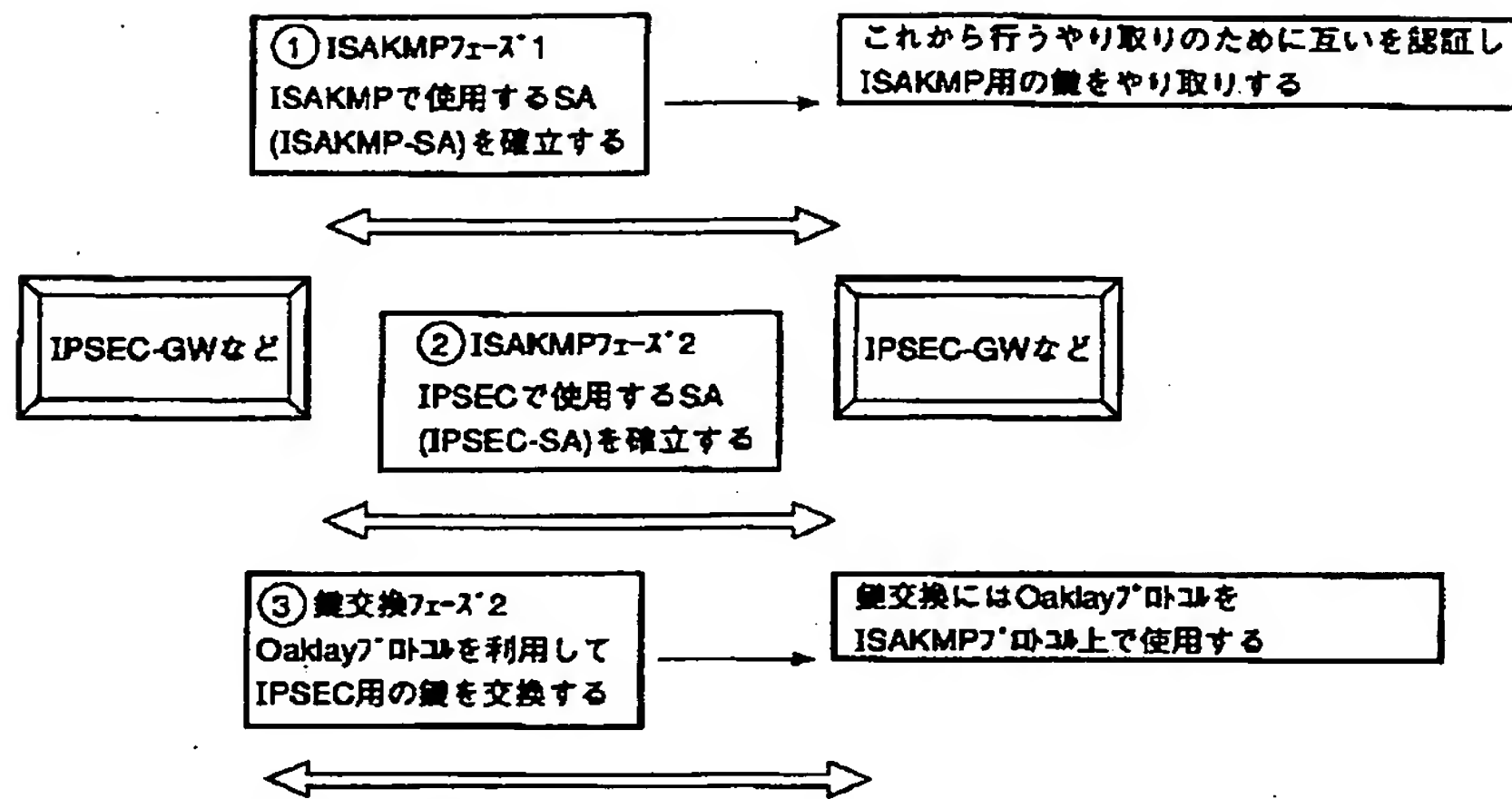
【図17】



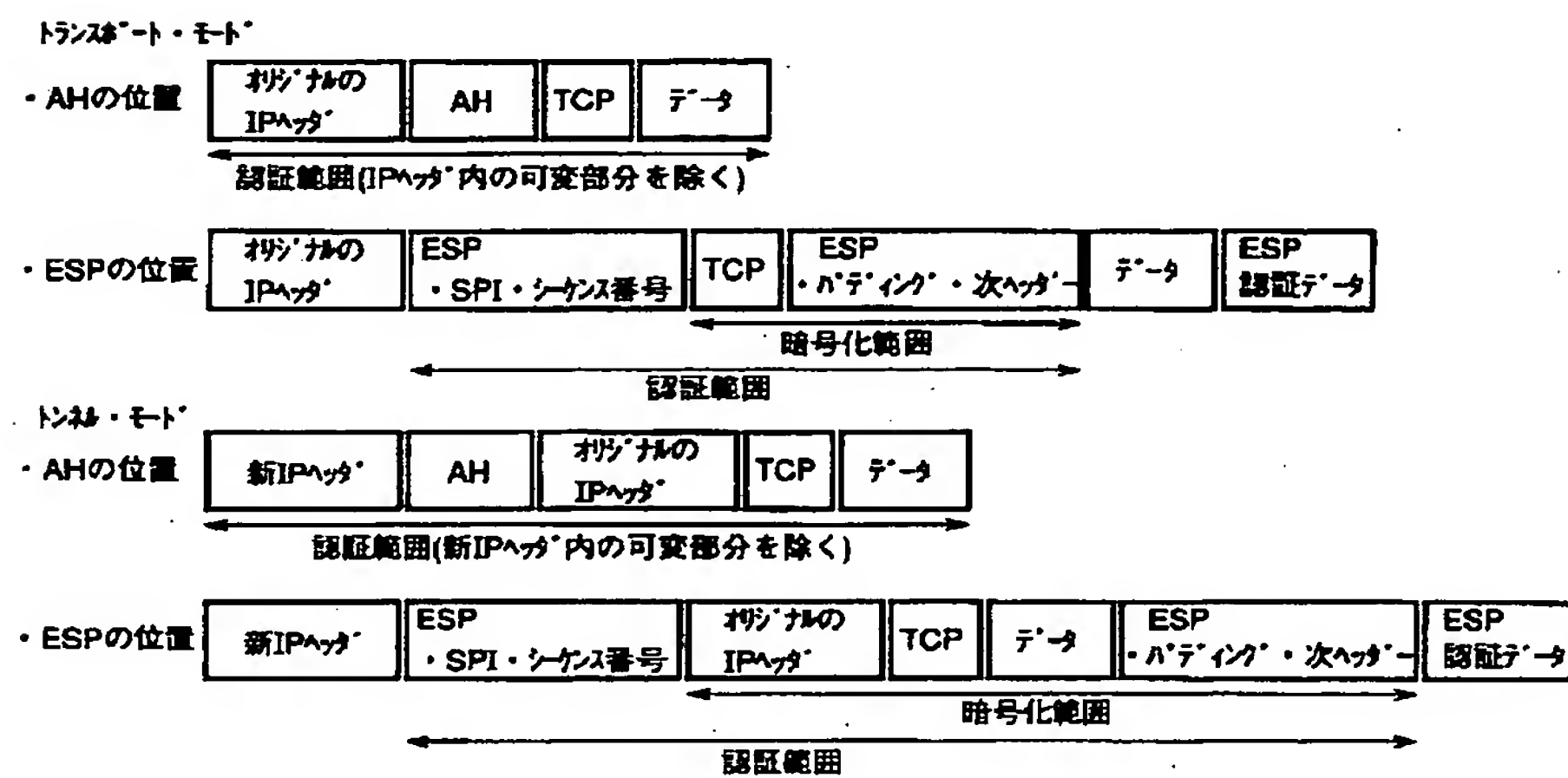
【図18】



【図19】



【図20】



フロントページの続き

(72)発明者 岸上 徹
東京都日野市旭が丘3丁目1番地の1 株
式会社東芝日野工場内

Fターム(参考) 5J104 AA01 AA07 AA16 BA02 EA20
KA02 NA21 PA07
5K030 GA15 HA08 HC14 HD03
5K033 AA08 CC01 DB14 DB18 EC03